

AN IDELIC VIEW OF IDEALS

SHIN-EUI SONG

ABSTRACT. Ideles and adeles can be viewed as a generalization of Minkowski theory, in which embedding of a number field to the Cartesian product of its completions at the archimedean valuation is generalized to an embedding of the Cartesian product of all its completions with some restriction.

This paper introduces the basic notions of point-set topology and builds the real numbers from the rational numbers. Then we review concepts from local fields that will lead to the product formula and the approximation theorem. We, then, construct adeles and ideles. The ideles modulo k^* maps surjectively to the ideal class group, and the compactness of C_S^0 will give rise to an alternative proof to the Dirichlet's S-unit theorem and the finiteness of ideal class group.

The paper assumes that the reader is familiar with Dedekind domain, principal ideal domain, unique factorization of Dedekind domain, and field norm and traces. The first few parts of Chapter 1 in Neukirch's *Algebraic Number Theory* will be sufficient for the paper.

CONTENTS

Notation	2
Part 1. Preliminaries	2
1. Point-set Topology	2
2. Construction of \mathbb{R}	5
Part 2. Local Fields	11
3. Abstract Valuation	11
4. Nonarchimedean valuation of k	17
5. Completion	21
6. Topology on local fields	29
7. Hensel's Lemma	33
8. Product Formula	35
Part 3. Adeles and Ideles	38
9. Restricted product	38
10. Finiteness and Unit Theorem	40
Appendices	46
Appendix A. Lemmas	46
Appendix B. Quotes	49
Index	50
References	51

NOTATION

Let F be an ordered field, then $F^{>0} := \{x \in F \mid x > 0\}$ and similarly $F^{\geq 0} := \{x \in F \mid x \geq 0\}$. We can also have $F^{<0}, F^{\leq 0}$ which is defined likewise.

Generally, F will denote an arbitrary field and k will denote a number field. Often K will be used as a field extension of both F and k .

Part 1. Preliminaries

We assume that the reader has learned the ideal-theoretic approach. The reader should have experience with Dedekind domains, discrete valuation ring, and the unique factorization into product of prime ideals.

1. POINT-SET TOPOLOGY

Let X be a topological space, then a **neighborhood** of $x \in X$ is a subset $V \subset X$ which contains an open set U containing x , i.e.

$$x \in U \subset V$$

The sequence $\{x_n\}$ in X is said to **converge** to $x \in X$ if for all open set $U \subset X$ containing x , there exists $N \in \mathbb{N}$ such that $x_n \in U$ whenever $n \geq N$. A topological space X is a **Hausdorff space** if for any two distinct points x_1 and x_2 in X , there exist two open sets U_1 and U_2 that contain x_1 and x_2 respectively, with $U_1 \cap U_2 = \emptyset$.

Proposition 1.1. *Let X be a Hausdorff space and let $\{x_n\}$ be a sequence in X , then $\{x_n\}$ converges to a unique limit point.*

Proof. Suppose that the sequence $\{x_n\}$ converges to x and x' , then there exists two disjoint open sets U_x and $U_{x'}$ containing x and x' respectively. However, there exist $N_1, N_2 \in \mathbb{N}$ such that

$$\begin{aligned} n \geq N_1 &\Rightarrow x_n \in U_x \\ n \geq N_2 &\Rightarrow x_n \in U_{x'} \end{aligned}$$

then $x_n \in U_x \cap U_{x'}$ for $n \geq \max(N_1, N_2)$, which contradicts that the two open sets are disjoint. Hence any convergent sequence converges to a unique point in a Hausdorff space. \square

A point x in a topological space X is called an **isolated point** of $S \subset X$ if there exists a neighborhood V of x with $V \cap S = \{x\}$. A **discrete set** is a subset of X consisting only of isolated points. Notice that if a topological space X has a discrete topology, one point subset $\{x\}$ of X is open. This is equivalent to saying that every point $x \in X$ is an isolated point of X . Hence we have that a subset $S \subset X$ is discrete if and only if S has a discrete topology as its subspace topology.

A **limit point** x of a set Y is a point where every neighborhood of x contains a point that is not x . A subset Y of a topological space X is called **dense** if either $x \in Y$ or x is a limit point in Y . Suppose U be an open set of X . Pick $x \in U$. If $x \notin Y$, then x is a limit point of Y . Clearly U is a neighborhood of x , hence there exists a point in U that is also in Y . Thus we have that $U \cap Y \neq \emptyset$ for every open set U of X .

Suppose we have two continuous mappings into a Hausdorff space Z , $f_1, f_2 : X \rightarrow Z$, and suppose that the map f_1 and f_2 coincide in some dense subset Y of X . Suppose that $f_1(y) \neq f_2(y)$, then there exists open sets U_1 and U_2 of Z containing $f_1(y)$ and $f_2(y)$ respectively that is disjoint. We have that $U = f_1^{-1}(U_1) \cap f_2^{-1}(U_2)$,

then by continuity, U is open. We have that $y \in U$, so U is not empty. Also, for any $y' \in U$,

$$f_1(y') \in U_1 \text{ and } f_2(y') \in U_2 \Rightarrow f_1(y') \neq f_2(y')$$

as $U_1 \cap U_2$ is empty. Thus f_1 and f_2 disagrees in all U , however, because $U \cap Y \neq \emptyset$, this leads to a contradiction.

Let (X, τ) be a topological space and \sim be an equivalence relation on X . Then we let $Y = X/\sim$ and give the topology on Y defined by

$$\tau_Y = \{U \subset Y \mid p^{-1}(U) \in \tau\}$$

where $p : X \rightarrow Y$ is the canonical epimorphism. Or equivalently,

$$\tau_Y = \{U \subset Y \mid \bigcup_{[x] \in U} [x] \in \tau\}$$

The space (Y, τ_Y) will be called the **quotient space** of X and τ_Y will be called the **quotient topology**.

Let X_i be a topological space and let

$$X = \prod_{i \in I} X_i$$

for some indexing set I with canonical projections $p_i : X \rightarrow X_i$. The **product topology** of X is defined to be the coarsest topology for which all p_i are continuous. This means that open sets of the form

$$p_i^{-1}(U_i) = U_i \times \prod_{j \in I, j \neq i} X_j$$

must be in the product topology. As a topology is closed under union and finite intersection, we can see that all open sets are unions of the form

$$\prod_{i \in S} U_i \times \prod_{i \notin S} X_i$$

where $S \subset I$ is a finite subset. The finiteness of S comes from the fact that the topology is only closed under finite intersection.

Let X be a topological space and $K \subset X$ be a subset of X . Then $\{U_\alpha\} \subset \tau$ is called an **open cover** for K if

$$K \subset \bigcup U_\alpha$$

and we say that $\{U_\alpha\}$ **covers** K . An **open subcover** of $\{U_\alpha\}$ is simply a subset that covers K . The space X is called **compact** if for any collection of open sets $\{U_\alpha\}$ which covers X , i.e.

$$X = \bigcup U_\alpha$$

there exists a finite collection $U_1, \dots, U_n \in \{U_\alpha\}$. Similarly, a subset $K \subset X$ is called **compact** if for any open cover for K , there exists a finite open subcover for K . Compactness is a global property in the sense that compact set is compact space in its own right. We give the following characterization.

Proposition 1.2. *K is a compact subset of X if and only if K is a compact space as a subspace of X .*

Proof. Let $K \subset X$ be a compact subset, and let $\{U'_\alpha\}$ be an open cover for K in the subspace topology. we have $U'_\alpha = U_\alpha \cap K$ for some open set U_α in X . So we see that $\{U_\alpha\}$ is an open cover of K in X . There exists a finite subcover $\{U_i\}_{i=1}^n$ by compactness. $\{U_i \cap K\}_{i=1}^n$ gives the desired finite subcover of $\{U'_\alpha\}$.

Conversely, let K be a compact subspace of X . If $\{U_\alpha\}$ is an open cover for K with $U_\alpha \subset X$ open, $\{U_\alpha \cap K\}$ is an open cover in the subspace topology and induces a finite subcover $\{U_i \cap K\}_{i=1}^n$ in the subspace topology. $\{U_i\}_{i=1}^n$ is a finite subcover of $\{U_\alpha\}$ for K . \square

Proposition 1.3. *Let S be a closed subset of a compact set K , then S is also compact.*

Proof. If $S = K$, then S is already compact. We may assume that $S \neq K$. Let $\{U_\alpha\}$ be an open cover for S , then $\{U_\alpha\} \cup \{S^c\}$ is an open cover for K . Then there exists $\{U_i\} \cup \{S^c\}_{i=1}^n$ a finite subcover. Because $S^c \cap S = \emptyset$, $\{U_i\}_{i=1}^n$ gives a subcover for S . \square

Proposition 1.4. *Let X be a compact space, then all its quotient space is also compact.*

Proof. Let Y be a quotient space of X , and let $\{U_\alpha\}$ be a open cover for Y , then by surjectivity, $\{q^{-1}(U_\alpha)\}$ is an open cover of X . Hence there exists a finite subcover $\{q^{-1}(U_i)\}_{i=1}^n$. So $\{q(q^{-1}(U_i))\}_{i=1}^n = \{U_i\}_{i=1}^n$ is a finite subcover of $\{U_\alpha\}$. \square

Proposition 1.5. *Let X be a discrete and compact space, then X has only finitely many points.*

Proof. If X is endowed with a discrete topology, then collection of all singletons $\{x\}$ for $x \in X$ is an open cover of X . As there exists a finite subcover, we immediately get X is finite. \square

Theorem 1.6 (Tychonoff). *Let $\{K_\alpha\}$ be any collection of compact spaces K_α , then*

$$\prod K_\alpha$$

is a compact space.

Let X be a topological space, then X is called **locally compact** if every point of X has a compact neighborhood. A compact space X is also locally compact, because for all point $x \in X$, the space X becomes the compact neighborhood of x .

Proposition 1.7. *Let X_1, \dots, X_n be locally compact spaces, then*

$$X = \prod_{i=1}^n X_i$$

is a locally compact space.

Proof. Let $(x_i)_{i=1}^n$ be a point in X , then for each x_i , there exists a compact neighborhood V_i and an open set U_i containing x_i such that $U_i \subset V_i$. Then

$$(x_i) \in \prod U_i \subset \prod V_i$$

then $\prod V_i$ is compact by Tychonoff's theorem and $\prod U_i$ is open in the product topology as it is a finite product. Hence (x_i) has a compact neighborhood. \square

Infinite product of locally compact spaces is not locally compact in general. By [9], we have that the only locally compact Hausdorff topological vector space are finite-dimensional. Infinite product of Hausdorff topological space over real cannot be finite-dimensional, so we see that it will never be locally compact. To resolve this problem, we will introduce the restricted product.

Let G be a group which is endowed with a topology. If the multiplication $*$: $G \times G \rightarrow G$ is continuous with $G \times G$ given a product topology and the inversion $^{-1} : G \rightarrow G$ is continuous, then G is called a **topological group**. If R is a ring endowed with a topology such that the addition $+$: $R \times R \rightarrow R$, negation $-$: $R \rightarrow R$, and multiplication $*$: $R \times R \rightarrow R$ are continuous then R is called a **topological ring**. Finally, a field F is called a **topological field** if F is a topological ring and, in addition, $^{-1} : F^\times \rightarrow F^\times$ is continuous. In short, a topological algebraic structure is a topological space if all its operations are continuous.

We now give an example of a locally compact topological field \mathbb{R} constructed from \mathbb{Q} and will prove the basic properties of \mathbb{R} .

2. CONSTRUCTION OF \mathbb{R}

One of the famous methods in completing the rational numbers \mathbb{Q} is to use Dedekind cuts, but in this paper we will use Cauchy sequences to fill in the gaps in the rational numbers. The following procedure generalizes to number fields and will be used to embed number fields to \mathbb{R}^n , the cartesian product of \mathbb{R} . Rational numbers will be denoted a, b to be distinguished with *real numbers* soon to be defined. The **absolute value** $| \cdot | : \mathbb{Q} \rightarrow \mathbb{Q}^{\geq 0}$ is defined by

$$|a| := \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0 \end{cases}$$

The absolute value satisfies the following well-known properties

Proposition 2.1. *Let $| \cdot |$ be the absolute value of \mathbb{Q} defined above, then*

- i) $|a| \geq 0$ and $|a| = 0$ if and only if $a = 0$,
- ii) $|ab| = |a||b|$,
- iii) $|a + b| \leq |a| + |b|$ (Triangle inequality)

We omit the tedious proof. A sequence $\{a_n\}_{n=1}^\infty$ or simply $\{a_n\}$ in \mathbb{Q} is called a **Cauchy sequence** if for any $\varepsilon \in \mathbb{Q}^{\geq 0}$, there exists a positive integer $N \in \mathbb{N}$ satisfying

$$|a_n - a_m| < \varepsilon \text{ whenever } n, m \geq N$$

the Cauchy sequence signifies that the terms grow closer together as the indices increase; however, there are Cauchy sequences that do not converge in a *non-complete* spaces. The construction of \mathbb{R} starts by constructing the ring of Cauchy sequence and embedding the rationals to the ring of Cauchy sequence of \mathbb{Q} and consider the quotient ring which turns out to field by modding out by the *nice* sequences.

Lemma 2.2. *Every Cauchy sequence $\{a_n\}$ is bounded, i.e. there exists $M \in \mathbb{Q}^{\geq 0}$ such that $|a_n| \leq M$ for all n .*

Proof. Let $\varepsilon = 1$, then we let $M = \max\{|a_n| \mid n \leq N_\varepsilon\} + 1$, then

$$\begin{aligned} |a_n| &\leq M && \text{if } n < N_\varepsilon \\ |a_n| &\leq |a_n - a_N| + |a_N| \\ &\leq 1 + (M - 1) \\ &= M && \text{if } n \geq N_\varepsilon \end{aligned}$$

□

Proposition 2.3. *Let $\{a_n\}$ and $\{b_n\}$ be Cauchy sequences, then so are $\{a_n + b_n\}$ and $\{a_n b_n\}$.*

Proof. For a fixed $\varepsilon \in \mathbb{Q}^{\geq 0}$, there exists N_1, N_2 such that

$$\begin{aligned} |a_n - a_m| &< \varepsilon/2 \quad \forall n, m \geq N_1 \\ |b_n - b_m| &< \varepsilon/2 \quad \forall n, m \geq N_2 \end{aligned}$$

then if we let $N = \max(N_1, N_2)$, then

$$|(a_n + b_n) - (a_m + b_m)| \leq |a_n - a_m| + |b_n - b_m| < \varepsilon/2 + \varepsilon/2 = \varepsilon$$

hence sum of Cauchy sequences is a Cauchy sequence.

For the product, we have that $|a_n|, |b_n| \leq B$ for some bound B , and for a fixed $\varepsilon \in \mathbb{Q}^{\geq 0}$, there exists N such that $|a_n - a_m|, |b_n - b_m| < \varepsilon/2B$ for all $n, m \geq N$. Then we get

$$\begin{aligned} |a_n b_n - a_m b_m| &= |a_n b_n - a_n b_m + a_n b_m - a_m b_m| \\ &\leq |a_n| |b_n - b_m| + |b_m| |a_n - a_m| \\ &\leq B \cdot \frac{\varepsilon}{2B} + B \cdot \frac{\varepsilon}{2B} = \varepsilon \end{aligned}$$

hence product of Cauchy sequences is a Cauchy sequence. □

The set of all Cauchy sequences \mathcal{R} is a ring. In fact, \mathcal{R} forms a subring of

$$\prod_{i=1}^{\infty} \mathbb{Q}$$

the countably infinite product of \mathbb{Q} . Let $A = \{a_n\} \in \mathcal{R}$ such that

$$a_n = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \neq 1 \end{cases}$$

and $B = \{b_n\} \in \mathcal{R}$ such that

$$b_n = \begin{cases} 1 & \text{if } n = 2 \\ 0 & \text{if } n \neq 2 \end{cases}$$

$AB = 0 \in \mathcal{R}$, hence we see that \mathcal{R} is not a domain.

Let $\mathcal{N} = \{A \in \mathcal{R} \mid a_n \rightarrow 0 \text{ as } n \rightarrow \infty\}$ be the set of all **null sequences**, a Cauchy sequence that converges to 0.

Proposition 2.4. *\mathcal{N} is an ideal of \mathcal{R}*

Proof. Let $B, C \in \mathcal{N}$, and $A \in \mathcal{R}$, with $B = \{b_n\}$ and $C = \{c_n\}$, then for any given $\varepsilon \in \mathbb{Q}^{\geq 0}$, there exist $N \in \mathbb{N}$ such that $n \geq N$ implies that

$$\begin{aligned} |b_n| &< \varepsilon/2 \\ |c_n| &< \varepsilon/2 \end{aligned}$$

hence $|b_n + c_n| \leq |b_n| + |c_n| < \varepsilon/2 + \varepsilon/2 = \varepsilon$. Hence $B + C \in \mathcal{N}$.

Also, let $A \in \mathcal{R}$, there exists $M \in \mathbb{Q}^{\geq 0}$ which bounds $|a_n|$, and there exists $N \in \mathbb{N}$ such that $|b_n| < \varepsilon/M$ whenever $n \geq N$, then for $n \geq N$,

$$\begin{aligned} |a_n b_n| &= |a_n| |b_n| \\ &\leq M |b_n| \\ &< \varepsilon \end{aligned}$$

This shows that $AB \in \mathcal{N}$, so \mathcal{N} is an ideal of \mathcal{R} . \square

Let $\mathbb{R} = \mathcal{R}/\mathcal{N}$, then we would like to discuss the nonzero element in \mathbb{R} . We will use $x, y \in \mathbb{R}$ for the elements and $x = [A]$ will denote the equivalence relation of $A \in \mathcal{R}$. If $A = \{a_n\}$, then we agree that $[a_n] := [A]$. Let $[A] \in \mathbb{R}$ be nonzero, then A is a Cauchy sequence that does not converge to 0. By taking the converse of the definition of convergence, we have

There exists $\varepsilon \in \mathbb{Q}^{\geq 0}$ such that for all $N \in \mathbb{N}$, there exists $M \geq N$ such that $|a_M| \geq \varepsilon$. (\dagger)

Proposition 2.5. *The composition*

$$\mathbb{Q} \hookrightarrow \mathcal{R} \twoheadrightarrow \mathbb{R}$$

is an inclusion and \mathbb{R} is a field.

Proof. Let $[a_n] \in \mathbb{R}$ nonzero. Fix $\varepsilon \in \mathbb{Q}^{\geq 0}$, then $\{a_n\}$ Cauchy implies that there exists N such that $|a_n - a_m| < \varepsilon$ whenever $n, m \geq N$. By (\dagger), there exists $M \geq N$ with $|a_M| > \varepsilon$. If we let $n \geq M$, then

$$||a_n| - |a_M|| \leq |a_n - a_M| < \varepsilon$$

implies that $-\varepsilon < |a_n| - |a_M| \Rightarrow 0 < |a_M| - \varepsilon < |a_n|$. ($\dagger\dagger$) Hence there exists N such that $|a_n| > 0$ for all $n \geq N$.

Let $[b_n]$ with $b_n = 0$ for $n < M$ and $b_n = a_n^{-1}$ for $n \geq M$. Then we get $[a_n][b_n] = [1]$. But we must first prove that $\{b_n\}$ is a Cauchy sequence. By the notation above, for all $n \geq NM$, we get

$$|a_M| - \varepsilon < |a_n| \Rightarrow \frac{1}{|a_n|} < \frac{1}{|a_M| - \varepsilon}$$

Let $B = 1/(|a_M| - \varepsilon)$, then for a fixed $\gamma \in \mathbb{Q}^{\geq 0}$, there exists $N \geq M$, such that

$$|x_n - x_m| < \varepsilon/B^2 \text{ whenever } n, m \geq N$$

which implies

$$|a_n^{-1} - a_m^{-1}| = \frac{|a_n - a_m|}{|a_n||a_m|} < \frac{\varepsilon}{B^2} \cdot B^2 = \varepsilon$$

This shows that $\{b_n\}$ is a Cauchy sequence. We have shown that every nonzero element in \mathbb{R} has a multiplicative inverse, hence \mathbb{R} is a field once we prove that $[1] \neq [0]$. But clearly $\{1\}$ does not converge to 0. Finally for any $a, b \in \mathbb{Q}$,

$$b \neq a \Rightarrow a - b \neq 0 \Rightarrow \{a - b\} \not\rightarrow 0 \Rightarrow [x - y] \neq 0$$

proves the injectivity of the composition. \square

We have extended \mathbb{Q} into a larger field \mathbb{R} using the absolute value $|\cdot|$. The absolute value can be also extended canonically to a function of \mathbb{R} as follows,

$$|\cdot| : \mathbb{R} \rightarrow \mathbb{R}$$

defined by

$$[a_n] \mapsto [|a_n|]$$

The inverse triangle inequality

$$||a_n| - |a_m|| \leq |a_n - a_m|$$

shows that $\{|a_n|\}$ is a Cauchy sequence. Also let $\{a_n\}$ be a null sequence, then $[a_n] = [0]$ as $||a_n| = |a_n|$, so the map is well-defined. One can check that the absolute value extended to \mathbb{R} satisfies the three properties stated in item iii) except for the first condition. In fact, we have not defined an order in \mathbb{R} . Suppose $x = [a_n] \in \mathbb{R}$ nonzero, then we know that $|a_n| - a_n = 0$ or $-2|a_n|$ and that there exists M such that $|a_n|$ is bounded below some $B \in \mathbb{Q}^{\geq 0}$ by $(\dagger\dagger)$ in 2.5. Let $\varepsilon < 2B$, then there exists N such that

$$||a_n| - a_n| - ||a_m| - a_m|| < \varepsilon \text{ whenever } n, m \geq N$$

this shows that for all $n \geq N$, $|a_n| - a_n = 0$ or $|a_n| - a_n = -2|a_n|$. The first case is when $|x| = x$ and the second case is when $|x| = -x$. Thus we have that the absolute value of \mathbb{R} is analogous to the case of \mathbb{Q} . We denote

$$\mathbb{R}^{\geq 0} := \{x \in \mathbb{R} \mid |x| = x\}$$

and it isn't hard to see that $\mathbb{Q}^{\geq 0} \subset \mathbb{R}^{\geq 0}$. We define $\mathbb{R}^{>0}$ similarly, and define elements in $\mathbb{R}^{>0}$ to be **positive** and elements in $\mathbb{R}^{<0}$ to be **negative**. From now on, when we say the absolute value of \mathbb{R} , then we mean $|\cdot| : \mathbb{R} \rightarrow \mathbb{R}^{\geq 0}$ such that

$$|x| = \begin{cases} x & \text{if } x \in \mathbb{R}^{\geq 0} \\ -x & \text{if } x \in \mathbb{R}^{<0} \end{cases}$$

Now \mathbb{R} becomes a metric space with the new absolute value $|\cdot|$. Cauchy sequence and convergence of \mathbb{R} is analogous to the case of \mathbb{Q} .

Proposition 2.6. *\mathbb{Q} is a dense subfield of \mathbb{R} .*

Proof. We identify \mathbb{Q} in \mathbb{R} as the image of \mathbb{Q} via the composition. Let $x = [a_n] \in \mathbb{R}$ with $\varepsilon \in \mathbb{Q}^{\geq 0}$. There exists N such that

$$|a_n - a_N| < \varepsilon \text{ whenever } n \geq N$$

If $r = a_N$, then we have $|a_n - r| < \varepsilon$ for all $n \geq N$ and thus $\varepsilon - |a_n - r| > 0$ for $n \geq N$. This shows that $[\varepsilon - |a_n - r|] \in \mathbb{R}^{\geq 0}$. Then

$$|x - [r]| \leq [\varepsilon]$$

Hence we have found for any $x \in \mathbb{R}$, there exists $r \in \mathbb{Q}$ such that $r \in [x - \varepsilon, x + \varepsilon]$. In other words, \mathbb{Q} is dense in \mathbb{R} . \square

The proposition above shows that the statements of the form “For a fixed $\varepsilon \in \mathbb{Q}^{\geq 0}$ ” can be replaced by “For a fixed $\varepsilon \in \mathbb{R}^{\geq 0}$ ” by denseness. A field is **Dedekind complete** if it satisfies the least upper bound property and is **Cauchy complete** if all Cauchy sequence converges. We will first prove that \mathbb{R} is Cauchy complete and prove that it is Dedekind complete.

Theorem 2.7. \mathbb{R} is Cauchy complete.

Proof. Let $\{a_n\} \in \mathcal{R}$, then we have $\{[a_n]\}$ a Cauchy sequence in \mathbb{R} . The definition of Cauchy sequence immediately implies that $\{[a_n]\} \rightarrow [a_n]$. Hence all rational Cauchy sequence converges in \mathbb{R} . Let $\{x_n\}$ be a Cauchy sequence in \mathbb{R} , then there exists $r_n \in \mathbb{Q}$ such that

$$|x_n - r_n| < 1/n$$

by denseness, hence $\lim_{n \rightarrow \infty} x_n - r_n = 0$. The convergence of $\{r_n\}$ implies the convergence of $\{x_n\}$. \square

Theorem 2.8. \mathbb{R} satisfies the least upper bound property.

Proposition 2.9 (Archimedean Property). *Let $x \in \mathbb{R}^*$, then for any $y \in \mathbb{R}$, there exists an integer n such that*

$$nx > y$$

Proposition 2.10. *Let $\alpha \in \mathbb{R}^{>0}$, then for all $x, y \in \mathbb{R}$, $x < y$ implies*

$$x^\alpha < y^\alpha$$

Theorem 2.11. \mathbb{R} is a locally compact topological space.

Proof. By Heine-Borel theorem, $x \in B(x, 1) \subset \overline{B(x, 1)}$, hence \mathbb{R} is a locally compact space. So we prove that the four operations $+, -, *, ^{-1}$ is continuous.

Let $f = +$, and $U = B(g, r)$. We fix $(a, b) \in f^{-1}(U)$ which shows that $|g - a - b| = r' < r$. There exists $\varepsilon > 0$ such that $r' + \varepsilon < r$. Now consider two open sets

$$U_1 = B(a, \varepsilon/2) \text{ and } U_2 = B(b, \varepsilon/2)$$

Let $(c, d) \in U_1 \times U_2$, then

$$\begin{aligned} |g - c - d| &= |g - a - b + a + b - c - d| \\ &\leq |g - a - b| + |a + b - c - d| \\ &< r' + \varepsilon/2 + \varepsilon/2 = r' + \varepsilon < r \end{aligned}$$

shows that $(a, b) \in U_1 \times U_2 \subset f^{-1}(U)$. $f^{-1}(U)$ is open and $+$ is continuous.

Let $f = -$, then for $B(x, r)$,

$$\begin{aligned} f^{-1}(B(x, r)) &= \{y \in \mathbb{R} \mid -y \in B(x, r)\} \\ &= \{y \in \mathbb{R} \mid |-y - x| < r\} \\ &= \{y \in \mathbb{R} \mid |(-x) - y| < r\} \\ &= B(-x, r) \end{aligned}$$

hence the preimage is open, and $-$ is continuous.

Let $f = *$ and $U = B(g, r)$ and fix $(a, b) \in f^{-1}(U)$. Let $|g - ab| = r'$ and we have $\varepsilon > 0$ such that $r' + \varepsilon < r$. We let $\varepsilon_1 = \min(\sqrt{\varepsilon}/\sqrt{3}, \varepsilon/3|b|)$ and $\varepsilon_2 = \min(\sqrt{\varepsilon}/\sqrt{3}, \varepsilon/3|a|)$. Consider two open sets

$$U_1 = B(a, \varepsilon_1) \text{ and } U_2 = B(b, \varepsilon_2)$$

then for all $(c, d) \in U_1 \times U_2$, we have $c = a + \gamma_1$ and $d = b + \gamma_2$ with $|\gamma_i| < \varepsilon_i$. We then have

$$\begin{aligned}
 |ab - cd| &= |ab - (a + \gamma_1)(b + \gamma_2)| \\
 &= |-a\gamma_2 - b\gamma_1 - \gamma_1\gamma_2| \\
 &\leq |a\gamma_2| + |b\gamma_1| + |\gamma_1\gamma_2| \\
 &< |a|\frac{\varepsilon}{3|a|} + |b|\frac{\varepsilon}{3|b|} + \frac{\sqrt{\varepsilon}\sqrt{\varepsilon}}{\sqrt{3}\sqrt{3}} \\
 &= \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon.
 \end{aligned}$$

We conclude by observing that

$$|g - cd| = |g - ab + ab - cd| \leq |g - ab| + |ab - cd| < r' + \varepsilon < r$$

which proves that $f^{-1}(U)$ is open.

Let $f = {}^{-1} : \mathbb{R}^* \rightarrow \mathbb{R}^*$ and $U = B(x, r)$, then fix $y \in f^{-1}(U)$, then consider

$$\gamma = \min \left(\frac{|y|}{2}, \frac{|y|^2}{2}\varepsilon \right)$$

with open set $B(y, \gamma)$. Similarly from above, we let $|x - y^{-1}| = r'$ and let $\varepsilon \in \mathbb{R}^{>0}$ such that $r' + \varepsilon < r$. Fix $z \in B(y, \gamma)$, then we have that

$$||z| - |y|| \leq |z - y| < \frac{|y|}{2}$$

implies that

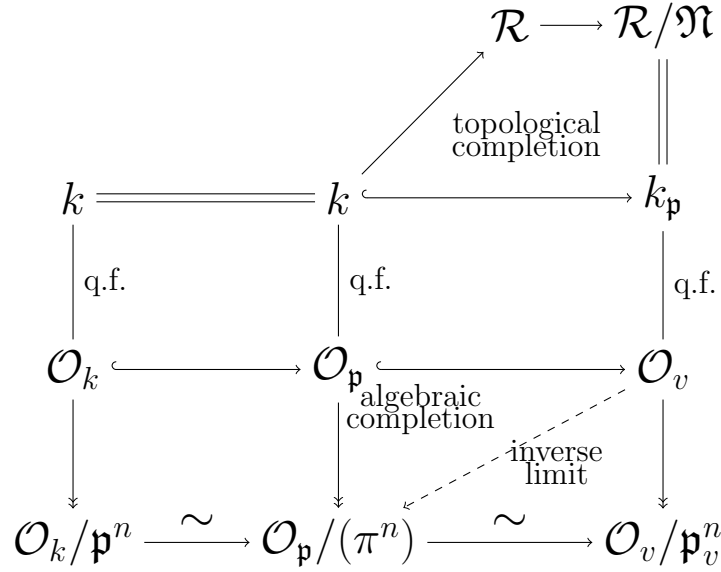
$$|y| - |z| < \frac{y}{2} \Rightarrow \frac{1}{2}|y| < |z| \Rightarrow \frac{1}{|z|} < \frac{2}{|y|}$$

The above inequality not gives us

$$\begin{aligned}
 |x - z^{-1}| &= |x - y^{-1} + y^{-1} - z^{-1}| \\
 &\leq |x - y^{-1}| + \frac{|y - z|}{\frac{|y||z|}{2}} \\
 &< r' + \left(\frac{2}{|y|} \right) \left(\frac{|y|^2}{2}\varepsilon \right) \left(\frac{1}{|y|} \right) \\
 &= r' + \varepsilon < r
 \end{aligned}$$

□

Part 2. Local Fields



k : number field

\mathcal{O}_k : the ring of integers of k

$\mathcal{O}_{\mathfrak{p}}$: the valuation ring of k with respect to $v_{\mathfrak{p}}$ or localization $(\mathcal{O}_k)_{\mathfrak{p}}$

\mathcal{O}_v : the inverse limit of $\mathcal{O}_{\mathfrak{p}}/(\pi^n)$, or the valuation ring of $k_{\mathfrak{p}}$

\mathcal{R} : ring of cauchy sequence of k ,

\mathfrak{N} : maximal ideal of R consisting of null sequences

$k_{\mathfrak{p}}$: completion of k with respect to $v_{\mathfrak{p}}$

\mathfrak{p} : prime ideal of \mathcal{O}_k

π : prime element of $\mathcal{O}_{\mathfrak{p}}$

\mathfrak{p}_v : the unique maximal ideal of \mathcal{O}_v

3. ABSTRACT VALUATION

A **valuation** of the field F is a function $\varphi : F \rightarrow \mathbb{R}^{\geq 0}$ satisfying

- i) $\varphi(x) = 0 \Leftrightarrow x = 0$,
- ii) $\varphi(xy) = \varphi(x)\varphi(y)$,
- iii) There exists C such that for any $x \in F$,

$$\varphi(x) \leq 1 \Rightarrow \varphi(1+x) \leq C \quad (1)$$

Let φ be a valuation such that $\varphi(x) = 0$ for $x = 0$ and $\varphi(x) = 1$ for all $x \in F^*$, then φ is called a **trivial valuation**. Also any valuation φ defines a homomorphism of $F^* \rightarrow \mathbb{R}^{>0}$, so we get $\varphi(1) = 1$.

$1 = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$. Dividing by $\varphi(x)$, $\varphi(x^{-1}) = \varphi(x)^{-1}$. Furthermore, $1 = \varphi(-1)\varphi(-1) = \varphi(-1)^2$, then $\varphi(-1) = 1$. Any root of unity in \mathbb{C} is of the form

$$\cos(2\pi m/n) + i \sin(2\pi m/n)$$

where $1 \leq m \leq n$. The number of the form above is real if and only if $\sin(2\pi m/n) = 0$ if and only if $\cos(2\pi m/n) = \pm 1$. Therefore, if ζ is a root of unity in F , $\varphi(\zeta) = 1$.

Let F be a finite field, then for nonzero $a \in F$, there exists $n \neq m$ positive integers such that $x^n = x^m$. However, $\varphi(x) > 0$ with $\varphi(x)^n \neq \varphi(a)^m$ whenever $n \neq m$. Hence, only valuation of a finite field F is the trivial valuation.

Proposition 3.1. (1) can be replaced by

$$\varphi(x + y) \leq C \max(\varphi(x), \varphi(y)) \quad (2)$$

Proof. Without loss of generosity, assume that $\varphi(x) \leq \varphi(y)$, then $\varphi(x/y) \leq 1 \Rightarrow \varphi(x/y + 1) \leq C$. Multiplying $\varphi(y)$ on both side we get

$$\varphi(x + y) \leq C\varphi(y) = C \max(\varphi(x), \varphi(y))$$

The case when $\varphi(y) \leq \varphi(x)$ is exactly the same.

Conversely, $\varphi(x) \leq 1$, then $\max(\varphi(x), \varphi(1)) = \varphi(1)$, so

$$\varphi(x + 1) \leq C \max(\varphi(x), \varphi(1)) = C$$

□

Lemma 3.2. If $\alpha \in \mathbb{R}^{>0}$ and φ be a valuation of F , then φ^α is also a valuation of F .

Proof.

- i) $\varphi^\alpha(x) = 0 \Leftrightarrow (\varphi(x))^\alpha = 0 \Leftrightarrow \varphi(x) = 0 \Leftrightarrow x = 0$,
- ii) $\varphi^\alpha(xy) = (\varphi(xy))^\alpha = (\varphi(x)\varphi(y))^\alpha = \varphi(x)^\alpha \varphi(y)^\alpha = \varphi^\alpha(x)\varphi^\alpha(y)$,
- iii) Let $C \in \mathbb{R}$ such that

$$\varphi(x) \leq 1 \Rightarrow \varphi(x + 1) \leq C$$

then

$$\varphi^\alpha(x) \leq 1 \Rightarrow \varphi(x)^\alpha \leq 1 \Rightarrow \varphi(x) \leq 1 \Rightarrow \varphi(x + 1) \leq C \Rightarrow \varphi(x + 1)^\alpha \leq C^\alpha \quad (3)$$

The last line shows that if C is a real number number that satisfies (1) for φ , then C^α satisfies (1) for φ^α .

□

If φ is a valuation of F , we define S_φ to be the set of all real numbers satisfying the condition (1), i.e.

$$S_\varphi := \{C \in \mathbb{R} \mid \varphi(x) \leq 1 \Rightarrow \varphi(1 + x) \leq C \text{ for all } x \in F\}$$

Then $1 = \varphi(1) = \varphi(1 + 0) \leq C$ shows that 1 is a lower bound of S_φ . Thus we may define the **norm** of a valuation denoted

$$\|\varphi\| = \inf S_\varphi$$

Proposition 3.3. Let $C = \|\varphi\|$, then $C \in S_\varphi$.

Proof. $C = \|\varphi\|$ implies that there exists a sequence of numbers D_n that converges to C . In fact, for each n , there exists $D_n \in S_\varphi$ such that $D_n - C < 1/n$, then $D_n \rightarrow C$. For any $\varphi(x) \leq 1$, we have that

$$\varphi(1 + x) \leq D_n$$

then $n \rightarrow \infty$, we get

$$\varphi(1 + x) \leq C$$

which exactly states that $C \in S_\varphi$.

□

Proposition 3.4. For all $\alpha \in \mathbb{R}^{>0}$, $\|\varphi^\alpha\| = \|\varphi\|^\alpha$.

Proof. If $C \in S_\varphi$, then by (3), $C^\alpha \in S_{\varphi^\alpha}$. Hence we get a canonical bijection between S_α and S_{φ^α} by

$$C \mapsto C^\alpha$$

- i) Let $\|\varphi\| = C$, for all $D \in S_{\varphi^\alpha}$, $D^{1/\alpha} \in S_\varphi \Rightarrow C^\alpha \leq D$, hence C^α is a lower bound of S_{φ^α} .
- ii) $C \in S_\varphi \Rightarrow S^\alpha \in S_{\varphi^\alpha}$.

This concludes that $\|\varphi\|^\alpha = \inf S_{\varphi^\alpha} = \|\varphi^\alpha\|$. \square

Lemma 3.5. *Let φ be a valuation of F , then*

$$\|\varphi\| \leq 2 \Rightarrow \varphi(x_1 + \cdots + x_n) \leq 2n \max(\varphi(x_1), \dots, \varphi(x_n))$$

Proof. $\|\varphi\| = 2$ implies that $\varphi(x_1 + x_2) \leq 2 \max(\varphi(x_1), \varphi(x_2))$, so by induction, we have

$$\varphi(x_1 + x_2 + \cdots + x_r) \leq 2^r \max(\varphi(x_1), \dots, \varphi(x_r))$$

then for any n , we have a unique r such that $2^r \leq n < 2^{r+1}$, then

$$\begin{aligned} \varphi(x_1 + \cdots + x_n) &= \varphi(x_1 + \cdots + x_n + 0 + \cdots + 0) \\ &\leq 2^{r+1} \max(\varphi(x_1), \dots, \varphi(x_n)) \\ &\leq 2n \max(\varphi(x_1), \dots, \varphi(x_n)) \end{aligned}$$

where we have added 0 in order to make it into 2^{r+1} terms. \square

Proposition 3.6. *Let φ be a function from F to $\mathbb{R}^{\geq 0}$ satisfying*

- i) $\varphi(x) = 0 \Leftrightarrow x = 0$,
- ii) $\varphi(xy) = \varphi(x)\varphi(y)$,

then we have that

$$\|\varphi\| \leq 2 \Leftrightarrow \varphi(x + y) \leq \varphi(x) + \varphi(y)$$

Proof. If the triangle equality holds,

$$\varphi(x + y) \leq \varphi(x) + \varphi(y) \leq \max(\varphi(x), \varphi(y)) + \max(\varphi(x), \varphi(y)) = 2 \max(\varphi(x), \varphi(y))$$

hence $\|\varphi\| \leq 2$.

Suppose $\|\varphi\| \leq 2$, then we observe

$$\begin{aligned} (\varphi(x + y))^n &= \varphi \left(x^n + \binom{n}{1} x^{n-1}y + \cdots + \binom{n}{n-1} xy^{n-1} + y^n \right) \\ &\leq 2(n+1) \max \left(\varphi \left(\binom{n}{i} x^{n-i} y^i \right) \right) \\ &\leq 2(n+1) \max \left(2 \binom{n}{i} \varphi(x)^{n-i} \varphi(y)^i \right) \\ &\leq 4(n+1) \sum_{i=1}^n \left(\binom{n}{i} \varphi(x)^{n-i} \varphi(y)^i \right) \\ &= 4(n+1) (\varphi(x) + \varphi(y))^n \end{aligned}$$

We take the n^{th} root and let $n \rightarrow \infty$, then we get the triangle inequality. \square

Theorem 3.7. *Let φ be a valuation of F and T_φ be a topology with the fundamental open sets*

$$B(x, \varepsilon) = \{y \in F \mid \varphi(x - y) < \varepsilon\}$$

then T_φ is a Hausdorff space.

Proof. Let φ be a valuation of F , then for any $\alpha \in \mathbb{R}^{>0}$, we have that the fundamental open sets of φ and φ^α are the same. In fact,

$$B_\varphi(x, \varepsilon) = \{y \in F \mid \varphi(x - y) < \varepsilon\} = \{y \in F \mid \varphi^\alpha(x - y) < \varepsilon^\alpha\} = B_{\varphi^\alpha}(x, \varepsilon^\alpha)$$

This shows that $T_\varphi = T_{\varphi^\alpha}$.

We can assume that φ satisfies the triangle inequality because if $\|\varphi\| > 2$, then we can always find $\alpha \in \mathbb{R}^{\geq 0}$ such that $\|\varphi^\alpha\| = \|\varphi\|^\alpha \leq 2$. We first show that the fundamental open sets is actually a basis.

- i) $x \in B(x, 1)$,
- ii) Let $y \in B(x, \varepsilon)$, with $\varphi(x - y) = \lambda$. Then we have $0 < \gamma < \varepsilon - \lambda$, so that for any $z \in (y, \gamma)$, we have that

$$\varphi(x - z) = \varphi(x - y + y - z) \leq \varphi(x - y) + \varphi(y - z) < \lambda + \varepsilon - \lambda = \varepsilon$$

For any two fundamental open sets $B(y_1, \varepsilon_1), B(y_2, \varepsilon_2)$, and a point $x \in B(y_1, \varepsilon_1) \cap B(y_2, \varepsilon_2)$, we just shown that there exists $B(x, \gamma_i) \subset B(y_i, \varepsilon_i)$. Furthermore, $x \in B(x, \gamma_1) \cap B(x, \gamma_2) = B(x, \gamma) \subset B(y_1, \varepsilon_1) \cap B(y_2, \varepsilon_2)$, where $\gamma = \min(\gamma_1, \gamma_2)$.

This shows that the fundamental open sets are indeed a basis and defines a topology on F . Now if x and y are two distinct points with $\varphi(x - y) = \varepsilon$, we have the two distinct open sets $B(x, \varepsilon/2)$ and $B(y, \varepsilon/2)$, for any z in the intersection, we have

$$\varepsilon = \varphi(x - y) = \varphi(x - z + z - y) \leq \varphi(x - z) + \varphi(z - y) < \varepsilon/2 + \varepsilon/2 = \varepsilon$$

which gives a contradiction. \square

A topology induced by a valuation φ will be always be denoted by T_φ . Viewing the field F as a topological space via T_φ , we have the following characterization of convergence.

$$x_n \rightarrow 0 \text{ in } T_\varphi \text{ if and only if } \varphi(x_n) \rightarrow 0 \text{ in } \mathbb{R}$$

For one direction, we have that fix $\varepsilon > 0$, then for because $B(0, \varepsilon)$ is an open set containing 0, there exists N such that $n \geq N \Rightarrow x_n \in B(0, \varepsilon)$. This is translated into

$$n \geq N \Rightarrow |\varphi(x_n) - 0| < \varepsilon$$

hence $\varphi(x_n) \rightarrow 0$ in \mathbb{R} .

Conversely, let U be an open set containing 0, then because 0 is an interior point of U . Hence there exists $\varepsilon > 0$ such that $0 \in B(0, \varepsilon) \subset U$. For this ε , there exists N such that

$$n \geq N \Rightarrow |\varphi(x_n)| < \varepsilon \Rightarrow x_n \in B(0, \varepsilon) \subset U$$

Hence the usual metric convergence is equivalent to the topological convergence. Furthermore, we know that in \mathbb{R} , we have

$$\varphi(x^n) \rightarrow 0 \text{ in } \mathbb{R} \Leftrightarrow \varphi(x) < 1 \Leftrightarrow x \in B(0, 1)$$

Theorem 3.8. *Let φ_1 and φ_2 be nontrivial valuations of F and $x \in F$ be arbitrary, then the following are equivalent*

- i) $\varphi_2 = \varphi_1^\alpha$ for some $\alpha \in \mathbb{R}^{\geq 0}$,
- ii) $T_{\varphi_1} = T_{\varphi_2}$,
- iii) $T_{\varphi_1} \supset T_{\varphi_2}$, i.e. T_{φ_1} is a stronger/finer topology than T_{φ_2} ,
- iv) $\varphi_1(x) < 1 \Rightarrow \varphi_2(x) < 1$,
- v) $\varphi_1(x) \leq 1 \Rightarrow \varphi_2(x) \leq 1$,

$$vi) \begin{cases} \varphi_1(x) < 1 & \Leftrightarrow \varphi_2(x) < 1 \\ \varphi_1(x) \leq 1 & \Leftrightarrow \varphi_2(x) \leq 1 \\ \varphi_1(x) > 1 & \Leftrightarrow \varphi_2(x) > 1 \end{cases}$$

Proof.

(i) \Rightarrow (ii):

$$\begin{aligned} B_2(x, r) &= \{y \in F \mid \varphi_2(x - y) < r\} = \{y \in F \mid \varphi_1^\alpha(x - y) < r\} \\ &= \{y \in F \mid \varphi_1(x - y) < r^{1/\alpha}\} = B_1(x, r^{1/\alpha}) \end{aligned}$$

The above shows that the fundamental open sets of both topology coincide, so two topologies coincide.

(ii) \Rightarrow (iii): Obvious

(iii) \Rightarrow (iv):

$$\varphi_1(x) < 1 \Rightarrow x \rightarrow 0 \text{ in } T_{\varphi_1}$$

which implies that any open set U in T_{φ_1} , there exists $n \geq N$ such that $x_n \in U$. Any open set in T_{φ_2} is an open set in T_{φ_1} , so the same criterion holds. This implies that

$$x \rightarrow 0 \text{ in } T_{\varphi_2} \Rightarrow \varphi_2(x) < 1$$

(iv) \Rightarrow (v): Suppose $\varphi_1(x) = 1$ and $\varphi_2(x) > 1$ for contradiction. Because φ_1 is nontrivial, there exists $y \in F$ such that $\varphi_1(y) < 1$, so $\varphi_2(y) < 1$. Because $\varphi_2(x) > 1$ there exists $n \in \mathbb{N}$ such that $\varphi_2(1/y) < \varphi_2(x)^n \Rightarrow 1 < \varphi_2(x^n y)$.

$$\varphi_1(x^n y) = \varphi_1(y) < 1 \Rightarrow \varphi_1(x^n y) < 1$$

gives a contradiction.

(v) \Rightarrow (vi): Now suppose $\varphi_1(x) < 1$ and $\varphi_2(x) = 1$ and let $y \in F$ such that $\varphi_2(y) > 1$. There exists $n \in \mathbb{N}$ such that

$$\varphi_1(x)^n \varphi_1(y) < 1 \Rightarrow \varphi_2(x^n y) < 1$$

but $\varphi_2(x^n y) = \varphi_2(y) > 1$, a contradiction. This shows that $\varphi_1(x) < 1 \Rightarrow \varphi_2(x) < 1$. The contrapositive of the assumption gives $\varphi_2(y) > 1 \Rightarrow \varphi_1(y) > 1$. Then we have

$$\varphi_1(x) > 1 \Rightarrow \varphi_1(1/x) < 1 \Rightarrow \varphi_2(1/x) < 1 \Rightarrow \varphi_2(x) > 1$$

$$\varphi_2(x) < 1 \Rightarrow \varphi_2(1/x) > 1 \Rightarrow \varphi_1(1/x) > 1 \Rightarrow \varphi_1(x) < 1$$

Thus it remains to show that

$$\varphi_1(x) = 1 \Leftrightarrow \varphi_2(x) = 1$$

But by the result above $\varphi_1(x) = 1 \Rightarrow \varphi_2(x) \geq 1$ and $\varphi_2(x) \leq 1$, hence $\varphi_2(x) = 1$. The analogue proof gives us the desired result.

(vi) \Rightarrow (i): The last proof uses the fact that \mathbb{Q} is dense in \mathbb{R} . Now let $x \in F$ such that $\varphi_1(x) > 1$, and thus $\varphi_2(x) > 1$, then we define

$$\alpha = \frac{\log \varphi_2(x)}{\log \varphi_1(x)}$$

and claim that

$$\varphi_2 = \varphi_1^\alpha$$

Suppose

$$\gamma_i = \frac{\log \varphi_i(y)}{\log \varphi_i(x)}$$

for any $y \in F$. If we could show that $\gamma_1 = \gamma_2$, then we show that $\log \varphi_1(y)/\log \varphi_2(y) = \log \varphi_2(x)/\log \varphi_1(x)$, hence for any $y \in F$,

$$\varphi_1(y)^\alpha = \varphi_1(y)^{\log \varphi_2(x)/\log \varphi_1(x)} = \varphi_1(y)^{\log \varphi_2(y)/\log \varphi_1(y)} = \varphi_2(y)$$

so it suffice to show that $\gamma_1 = \gamma_2$. Now let m/n be a rational number such that $m/n \geq \gamma_1$, then

$$\begin{aligned} m/n \geq \gamma_1 &\Leftrightarrow m \log \varphi_1(x) \geq n \log \varphi_1(y) \\ &\Leftrightarrow \varphi_1(x^m) \geq \varphi_1(y^n) \\ &\Leftrightarrow \varphi_1(x^m/y^n) \geq 1 \\ &\Leftrightarrow \varphi_2(x^m/y^n) \geq 2 \\ &\Leftrightarrow \varphi_2(x^m) \geq \varphi_2(y^n) \\ &\Leftrightarrow m \log \varphi_2(x) \geq n \log \varphi_2(y) \\ &\Leftrightarrow m/n \geq \gamma_2 \end{aligned}$$

Performing the same procedure, we get $m/n \leq \gamma_1 \Rightarrow m/n \leq \gamma_2$. By the denseness of \mathbb{Q} , we can always find sequences of \mathbb{Q} $\{q_i\}$ from above and $\{t_i\}$ from below that converge to γ_1 . We clearly have that

$$t_i \leq \gamma_2 \leq q_i$$

with $\lim_{i \rightarrow \infty} t_i = \lim_{i \rightarrow \infty} q_i = \gamma_1$ gives that $\gamma_2 = \gamma_1$ by comparison theorem. \square

Two nontrivial valuations are **equivalent** if the two induces the same topology. This is clearly a equivalence relation, and by the theorem, we have that its equivalence class is

$$\mathfrak{p} = [\varphi] = \{\varphi' \mid T_\varphi = T_{\varphi'}\} = \{\varphi' \mid \varphi' = \varphi^\alpha \text{ for some } \alpha \in \mathbb{R}^{\geq 0}\}$$

The equivalence class of valuations are called a **place**, but, in the case of number theory, places will be called the **prime divisor**. The deep connection between the primes and the places will be established in the next section.

Let φ and φ' be two equivalent valuations, then $\varphi' = \varphi^\alpha$. Then we have that

$$\|\varphi'\| > 1 \Leftrightarrow \|\varphi\|^\alpha > 1 \Leftrightarrow \|\varphi\| > 1^{1/\alpha} = 1$$

and similarly,

$$\|\varphi'\| = 1 \Leftrightarrow \|\varphi\| = 1$$

Let \mathfrak{p} be a prime divisor of F , then \mathfrak{p} is called **archimedean** if $\|\varphi\| > 1$ for all $\varphi \in \mathfrak{p}$. \mathfrak{p} is called **nonarchimedean** if $\|\varphi\| = 1$ for all $\varphi \in \mathfrak{p}$. Our next goal in this paper will be classifying all prime divisors in a number field k . The above remark shows that prime divisors are either archimedean or nonarchimedean.

Let K, F be fields with a field embedding $\mu : F \rightarrow K$. Then for any valuation φ of K ,

$$\varphi^\mu = \varphi \circ \mu$$

is easily verified to be a valuation of F . Furthermore, if $\alpha \in \mathbb{R}^{>0}$, then

$$(\varphi^\alpha)^\mu(x) = \varphi(\mu(x))^\alpha = (\varphi^\mu)^\alpha$$

hence sends equivalent valuations to equivalent valuations. Hence μ induces a map μ^* sending prime divisors of K to prime divisors of F by composing with the valuations of K .

Let $\mu : F \rightarrow K$ be a field embedding with \mathfrak{q} a prime divisor of K . Let $\mathfrak{p} := \mu^*(\mathfrak{q})$, then μ becomes a topological mapping between the topological spaces $(F, T_{\mathfrak{p}})$ and $(K, T_{\mathfrak{q}})$. We may view F as a subspace of K viewing the homeomorphism $F \cong \mu(F)$, hence the field embedding can be viewed as a topological embedding, thus continuous. In fact, we have $\varphi = \psi \circ \mu$ for some $\psi \in \mathfrak{q}$ and $\varphi \in \mathfrak{p}$. $\psi(x - y) < \varepsilon \Rightarrow \psi(\mu(x) - \mu(y)) < \varepsilon$. Furthermore, this shows that

$$\{x_n\} \text{ Cauchy/null sequence in } F \Rightarrow \{\mu(x_n)\} \text{ Cauchy/null sequence in } K$$

4. NONARCHIMEDEAN VALUATION OF k

A valuation of a number field k will be sometimes called a **multiplicative valuation** or an **absolute value** because the concept of valuation is a generalization of the usual absolute value of \mathbb{Q} . From now on F will denote arbitrary field, and k will denote number field.

Proposition 4.1. *Let φ be a valuation of an arbitrary field F , then the following are equivalent*

- i) $\mathfrak{p} = [\varphi]$ is nonarchimedean,
- ii) $\varphi(x + y) \leq \max(\varphi(x), \varphi(y))$ for all $x, y \in F$,
- iii) $\{\varphi(n \cdot 1) \mid n \in \mathbb{Z}\}$ is bounded.

Proof. The equivalence of i) and ii) are clear from previous remarks. So we assume ii). Then by induction we have that

$$\varphi(x_1 + \cdots + x_n) \leq \max(\varphi(x_1), \dots, \varphi(x_n))$$

Then $\varphi(n \cdot 1) \leq \varphi(1)$ which is bounded above $\varphi(1)$.

Now assume iii), then for all n , we have $\varphi(n) \leq M$ for some M .

$$\begin{aligned} [\varphi(x + y)]^n &\leq \varphi((x + y)^n) \\ &= \varphi\left(\sum_{i=1}^n \binom{n}{i} x^i y^{n-i}\right) \\ &\leq 2(n + 1) \max\left[\varphi\left(\binom{n}{i} x^i y^{n-i}\right)\right] \\ &\leq 2(n + 1)M \max(\varphi(x)^i \varphi(y)^{n-i}) \\ &\leq 2(n + 1)M \varphi(x)^n \end{aligned}$$

where in the last inequality, we assumed that $\varphi(x) \geq \varphi(y)$, then by taking the n^{th} root of unity, we get

$$\varphi(x + y) \leq \sqrt[n]{2(n + 1)M \varphi(x)} = \sqrt[n]{2(n + 1)M} \max(\varphi(x), \varphi(y))$$

taking $n \rightarrow \infty$, we see that

$$\varphi(x + y) \leq \max(\varphi(x), \varphi(y))$$

□

Now our task is to classify all nonarchimedean prime divisors of \mathbb{Q} . We first introduce another form of valuation that resembles the properties of the logarithmic function. An **exponential valuation** of F is a function $v : F \rightarrow \mathbb{R} \cup \{\infty\}$ satisfying,

- i) $v(x) = \infty \Leftrightarrow x = 0$,
- ii) $v(xy) = v(x)v(y)$,
- iii) $v(x + y) \geq \min(v(x), v(y))$.

First note that v induces a homomorphism $v : F^* \rightarrow \mathbb{R}$ with $v(F^*)$ a subgroup of additive group \mathbb{R} . Let $G \subset \mathbb{R}$ be a subgroup and suppose that G is not discrete, then there exists $x \in G$ that is not an isolated point. This means that for all $\varepsilon \in \mathbb{R}^{>0}$, there exists $y_\varepsilon \in G$ such that $|x - y_\varepsilon| < \varepsilon$. This is again tantamount to saying that for all $\varepsilon \in \mathbb{R}^{>0}$, there exists $0 < y_\varepsilon < \varepsilon$ such that $x \pm y_\varepsilon \in G$. Let $z \in \mathbb{R} \setminus G$ with a fixed $\varepsilon \in \mathbb{R}^{>0}$. We would like to show that $B(z, \varepsilon) \cap G \neq \emptyset$. By the archimedean property we have $n \in \mathbb{N}$,

$$nx \leq y < nx + |x|$$

then if $z - nx < \varepsilon$, then $nx \in B(z, \varepsilon) \cap G$. So we suppose that $z - nx = \delta > \varepsilon$. There exists $0 < y_\varepsilon < \varepsilon$ and m such that $my_\varepsilon < \delta < (m+1)y_\varepsilon$, so that

$$0 \leq \delta - my_\varepsilon < y_\varepsilon < \varepsilon$$

so

$$|nx + my_\varepsilon - z| = |my_\varepsilon - \delta| < \varepsilon$$

So we may conclude that $nx + my_\varepsilon \in B(0, \varepsilon)$, so G is dense in \mathbb{R} . We thus showed that any subgroup of \mathbb{R} is either discrete or dense in \mathbb{R} . We call an exponential valuation v **discrete** if $v(F^*)$ is a discrete subgroup of \mathbb{R} .

Furthermore, if G is a discrete subgroup of \mathbb{R} , and suppose $G \neq 0$, then there exists $s \in \mathbb{R}$ where s is the smallest positive number in G . Unless, 0 is not an isolated point in G . Now suppose there exists $t \in G$, such that $t \neq ns$ for all $n \in \mathbb{Z}$, then for some n , we have

$$ns < t < (n+1)s$$

with $0 < t - ns < s$ contradicting the minimality of s . Hence all discrete subgroup of \mathbb{R} is of the form $s\mathbb{Z}$. The discrete exponential valuation v is **normalized** if $v(F^*) = \mathbb{Z}$ meaning that $s = 1$.

The exponential valuation of \mathbb{Q} arises from observing the fundamental theorem of arithmetic and extending to \mathbb{Q} , but because our main goal is to study \mathcal{O}_k , we give a generalized construction using the unique factorization of ideals. For a fixed \mathfrak{p} a prime ideal of \mathcal{O}_k , for all fractional \mathfrak{A} of \mathcal{O}_k , we have the decomposition

$$\mathfrak{A} = \prod_{\substack{q \\ \text{prime ideal}}} \mathfrak{q}^{e_q(\mathfrak{A})}$$

We get a map $\tilde{v}_{\mathfrak{p}} : J_k \rightarrow \mathbb{Z}$ defined by $\mathfrak{A} \mapsto e_{\mathfrak{p}}(\mathfrak{A})$ where J_k is the group of fractional ideals of \mathcal{O}_k . This map induces a map $v_{\mathfrak{p}} : k \rightarrow \mathbb{Z} \cup \{\infty\}$ by the composition

$$k^* \rightarrow P_k \hookrightarrow J_k \xrightarrow{\tilde{v}_{\mathfrak{p}}} \mathbb{Z}$$

with $0 \mapsto \infty$. Suppose $x, y \in F$ with

$$(x) = \prod \mathfrak{p}^{e_{\mathfrak{p}}} \quad (y) = \prod \mathfrak{p}^{f_{\mathfrak{p}}}$$

where (x) denotes the fractional ideal generated by x , then

- i) $v_{\mathfrak{p}}(x) = \infty \Leftrightarrow x = 0$ by construction,

ii) We observe that

$$(xy) = (x)(y) = \prod_{\mathfrak{p} \text{ prime ideal}} \mathfrak{p}^{e_{\mathfrak{p}} + f_{\mathfrak{p}}}$$

clearly shows that $v_{\mathfrak{p}}(xy) = v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(y)$.

iii) We may assume that $e_{\mathfrak{p}} \leq f_{\mathfrak{p}}$, with $n = e_{\mathfrak{p}}$, then we have that

$$x, y \in \mathfrak{p}^n \Rightarrow x + y \in \mathfrak{p}^n$$

We get the desired result that $v_{\mathfrak{p}}(x + y) \geq v_{\mathfrak{p}}(x) = \min(v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y))$.

Let v be an exponential valuation of F , then we may choose $q > 1$ and define $\varphi_v : F \rightarrow \mathbb{R}^{\geq 0}$ by

$$x \mapsto q^{-v(x)}$$

which is, in fact, a nonarchimedean valuation of F . Conversely, for any nonarchimedean valuation φ of F , we can define an exponential valuation $v_{\varphi} : F \rightarrow \mathbb{R} \cup \{\infty\}$

$$x \mapsto -\log \varphi(x)$$

By the remark above, we see that there exists a canonical bijection $v \leftrightarrow \varphi$, and for a fixed $q > 1$, we see that another bijection $v^{\alpha} \leftrightarrow \varphi^{\alpha}$. So we will interchangeably use $v \in \mathfrak{p}$ and $\varphi \in \mathfrak{p}$ for nonarchimedean prime divisor \mathfrak{p} .

Lemma 4.2. *Let v be a nonarchimedean exponential valuation of a number field k , then*

$$v = sv_{\mathfrak{p}}$$

for some $s \in \mathbb{R}^{>0}$ and a unique nonzero prime ideal \mathfrak{p} .

Proof. We first prove existence of such \mathfrak{p} . Let

$$\mathfrak{p} := \{\alpha \in \mathcal{O}_k \mid v(\alpha) > 0\}$$

We have that $v(\alpha) = \infty > 0$, and $v(1) = v(1) + v(1) \Rightarrow v(1) = 0$. Also, $v(1) = v(-1 \cdot -1) = 2v(-1) \Rightarrow v(-1) = 0$. For any $n \in \mathbb{Z}$, $v(n) \geq v(1) = 0$.

Now let $\alpha \in \mathcal{O}_k$ nonzero, then by definition, there exists an equation

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$$

with n smallest possible, $a_i \in \mathbb{Z}$. Moving the lower terms to the other side, we get

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0$$

Let $0 \leq j < n$ with $a_j \neq 0$,

$$v(-a_j\alpha^j) \geq jv(\alpha)$$

If $v(\alpha) > 0$,

$$v(\alpha^n) \geq v(-a_{n-1}\alpha^{n-1} - \cdots - a_0) \geq v(-a_j\alpha^j) \geq jv(\alpha) \geq (n-1)v(\alpha)$$

and we have $nv(\alpha) = v(\alpha^n)$, so we get

$$nv(\alpha) \geq (n-1)v(\alpha) \Rightarrow v(\alpha) \geq 0$$

which yields a contradiction. This proves that for all $\alpha \in \mathcal{O}_k$, $v(\alpha) \geq 0$.

Next step is to show that \mathfrak{p} is a prime ideal. But this is easy to see as $x, y \in \mathfrak{p}$, $v(x + y) \geq \min(v(x), v(y)) > 0$, hence $x + y \in \mathfrak{p}$, and for all $x \in \mathcal{O}_k$ and $y \in \mathfrak{p}$, we have $v(x) \geq 0$, $v(y) > 0$. $v(xy) = v(x) + v(y) > 0$. Finally, v is not identically 0 for k^* because v is not trivial. v is not identically 0 for all $\mathcal{O}_k \setminus \{0\}$. In fact, if it was, then for any $x/y \in k^*$, $v(x/y) = v(x) - v(y) = 0 - 0 = 0$. We have shown that \mathfrak{p} is

nonzero.

Suppose $v_{\mathfrak{p}}(\alpha) = 0$, then we will show that $v(\alpha) = 0$. To prove this we need another lemma.

Lemma 4.3. *Let $\mathfrak{p} \subset \mathcal{O}_k$ be a prime ideal with $\alpha \in k^*$, then $\alpha = a/b$ with $v_{\mathfrak{p}}(b) = 0$ for some $a, b \in \mathcal{O}_k$.*

Proof. Let $(\alpha) = \mathfrak{A}\mathfrak{B}^{-1}$ where $\mathfrak{A}, \mathfrak{B}$ is an ideal of \mathcal{O}_k with $(\mathfrak{A}, \mathfrak{B}) = \mathcal{O}_k$, i.e. relatively prime. Then we have $v_{\mathfrak{p}}(\mathfrak{B}) = 0$ as $v_{\mathfrak{p}}(\alpha) \geq 0$. Because $\mathfrak{B}(\alpha) = \mathfrak{A}$, we have that $[\mathfrak{A}] = [\mathfrak{B}]$, where $[\]$ denotes the ideal class.

Let $[\mathfrak{A}]$ be any arbitrary ideal class, then \mathfrak{A} has a unique decomposition,

$$\mathfrak{A} = \prod_{i=1}^n \mathfrak{p}^{e_{p_i}}$$

with $e_{p_i} \in \mathbb{Z}$. Now fix a \mathfrak{p} prime ideal with and let $\pi \in \mathfrak{p}^m \setminus \mathfrak{p}^{m+1}$, then we have

$$(\pi) = \mathfrak{p}^m \prod \mathfrak{q}^{f_{q_i}}$$

where $m = e_{p_i}$. By chinese remainder theorem, we have an element x relatively prime to \mathfrak{p} and divisible by $\mathfrak{p}_i, \mathfrak{q}_i$ that is not \mathfrak{p} , then taking sufficiently large l , we get

$$(\pi^{-1}x^l)\mathfrak{A}$$

represents $[\mathfrak{A}]$, is an integral ideal, and is relatively prime to \mathfrak{p} .

Let $\mathfrak{C} \in [\mathfrak{A}]^{-1} = [\mathfrak{B}]^{-1}$ with \mathfrak{C} an integral ideal relatively prime to \mathfrak{p} , then we get

$$(\alpha) = \mathfrak{A}\mathfrak{C}(\mathfrak{B}\mathfrak{C})^{-1}$$

$\mathfrak{A}\mathfrak{C} = (a), \mathfrak{B}\mathfrak{C} = (b)$ giving us

$$\alpha = \frac{a}{b}$$

with $v_{\mathfrak{p}}(b) = 0$ as both $\mathfrak{B}, \mathfrak{C}$ are relatively prime to \mathfrak{p} . □

By the lemma, we easily get

$$v_{\mathfrak{p}}(\alpha) = v_{\mathfrak{p}}(a/b) = v_{\mathfrak{p}}(a) - v_{\mathfrak{p}}(b) = v_{\mathfrak{p}}(a) = 0$$

$a, b \in \mathcal{O}_k$ and $a, b \notin \mathfrak{p}$, we have $v(a) = v(b) = 0$ by definition. For any $\alpha \in k^*$, $n = v_{\mathfrak{p}}(\alpha) \in \mathbb{Z}$, and for $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, we get $v_{\mathfrak{p}}(\pi) = 1$. $v_{\mathfrak{p}}(\alpha\pi^{-n}) = 0$, so $v(\alpha\pi^{-n}) = 0$.

$$v(\alpha) = v(\pi^n) = v(\pi)n = v(\pi)v_{\mathfrak{p}}(\alpha)$$

Let $s = v(\pi)$ which is positive as $\pi \in \mathfrak{p}$, we get the desired result.

Now for uniqueness, let $v = s_1v_{\mathfrak{p}_1} = s_2v_{\mathfrak{p}_2}$, then

$$\begin{aligned} \mathfrak{p}_1 &= \{\alpha \in \mathcal{O}_k \mid v_{\mathfrak{p}_1}(\alpha) > 0\} = \{\alpha \in \mathcal{O}_k \mid s_1v_{\mathfrak{p}_1}(\alpha) > 0\} \\ &= \{\alpha \in \mathcal{O}_k \mid s_2v_{\mathfrak{p}_2}(\alpha) > 0\} = \{\alpha \in \mathcal{O}_k \mid v_{\mathfrak{p}_2}(\alpha) > 0\} = \mathfrak{p}_2 \end{aligned}$$

hence the prime ideal \mathfrak{p} is unique. □

We thus have shown that the only nonarchimedean prime divisor \mathfrak{p} of a number field k is $[v_{\mathfrak{p}}]$. Our next goal would be to classify all archimedean valuations of k , but we need completion which is a generalized technique used to construct the real numbers from \mathbb{Q} .

5. COMPLETION

Let \mathfrak{p} be a prime divisor of a field F , then a \mathfrak{p} -Cauchy sequence is a sequence $\{x_n\}$ in F such that

$$x_n - x_m \rightarrow 0 \text{ as } n, m \rightarrow \infty \text{ in } T_{\mathfrak{p}}$$

F is said to be **\mathfrak{p} -complete** if all \mathfrak{p} -Cauchy sequences converge. A field extension \widehat{F} of F with a prime $\widehat{\mathfrak{p}}$ with a field embedding $\mu : F \rightarrow \widehat{F}$ is said to be a **\mathfrak{p} -completion** of F if

- i) $F \subset \widehat{F}$,
- ii) $\mu(F) \subset \widehat{F}$ is dense,
- iii) $(\widehat{F}, \widehat{\mathfrak{p}})$ is $\widehat{\mathfrak{p}}$ -complete.

Notice that once we have found \widehat{F} satisfying ii) and iii), we may use set-theoretical trick to make \widehat{F} into an extension of F . We find S which is a set bijective to $\widehat{F} - F$ with respect to a bijection ψ . Let $\widetilde{F} = S \cup F$, then the bijection ψ can be extended to $\Psi : \widehat{F} \rightarrow \widetilde{F}$. Then \widetilde{F} is an extension of F by for all $x, y \in \widetilde{F}$,

$$xy := \Psi(\Psi^{-1}(x)\Psi^{-1}(y)) \text{ and } x + y := \Psi(\Psi^{-1}(x) + \Psi^{-1}(y))$$

Theorem 5.1. *Let F be a field with a prime divisor \mathfrak{p} . A \mathfrak{p} -completion of F exists, and it is essentially unique. In other words, if*

$$(\widehat{F}_1, \widehat{\mathfrak{p}}_1, \mu_1) \text{ and } (\widehat{F}_2, \widehat{\mathfrak{p}}_2, \mu_2)$$

are two \mathfrak{p} -completions of F , then there exists an unique isomorphism

$$\sigma : \widehat{F}_1 \rightarrow \widehat{F}_2$$

which is an extension of $1_F : F \rightarrow F$ such that $\sigma^(\widehat{\mathfrak{p}}_2) = \widehat{\mathfrak{p}}_1$.*

Proof. We choose $\varphi \in \mathfrak{p}$ such that $\|\varphi\| \leq 2$. In other words, φ satisfies the triangle inequality. We let \mathcal{R} be the set of all \mathfrak{p} -Cauchy sequences in F , then addition and multiplication defined componentwise makes \mathcal{R} into a ring as seen in 2.3. Let $X = \{x_n\} \in \mathcal{R}$, then there exists a canonical way to extend φ by putting

$$\widetilde{\varphi}(X) = \lim_{n \rightarrow \infty} \varphi(x_n)$$

then the reverse triangle inequality A.1 shows that the $\varphi(x_n)$ is Cauchy,

$$|\varphi(x_n) - \varphi(x_m)| \leq \varphi(x_n - x_m)$$

and the fact that \mathbb{R} is complete shows that the limit converges. We can easily see that for any $X, Y \in \mathcal{R}$,

- i) $\widetilde{\varphi}(X) \geq 0$, as $\varphi(x_n) \geq 0$ for all n .
- ii) $\widetilde{\varphi}(XY) = \widetilde{\varphi}(x)\widetilde{\varphi}(Y)$, as

$$\widetilde{\varphi}(XY) = \lim_{n \rightarrow \infty} \varphi(x_n)\varphi(y_n) = \lim_{n \rightarrow \infty} \varphi(x_n) \lim_{n \rightarrow \infty} \varphi(y_n) = \widetilde{\varphi}(X)\widetilde{\varphi}(Y)$$

- iii) $\widetilde{\varphi}(X + Y) \leq \widetilde{\varphi}(X) + \widetilde{\varphi}(Y)$ as

$$\widetilde{\varphi}(X + Y) = \lim_{n \rightarrow \infty} \varphi(x_n + y_n) \leq \lim_{n \rightarrow \infty} \varphi(x_n) + \varphi(y_n) = \widetilde{\varphi}(X) + \widetilde{\varphi}(Y)$$

hence $\tilde{\varphi}$ defines a valuation of \mathcal{R} . Next we define the subset of \mathcal{N} of \mathcal{R} by

$$\mathcal{N} := \{X \in \mathcal{R} \mid X = \{x_n\}, \lim_{n \rightarrow \infty} \varphi(x_n) = 0\}$$

called the **null sequences** of F . We define $\hat{F} := \mathcal{R}/\mathcal{N}$ and see that it is a field is proven similarly to 2.5. Also, let $N \in \mathcal{N}$ be a null sequence, then we have

$$\tilde{\varphi}(A) \leq \tilde{\varphi}(A + N) + \tilde{\varphi}(N) = \tilde{\varphi}(A + N) \leq \tilde{\varphi}(A)$$

shows that $\tilde{\varphi}$ is well-defined for the cosets of the form $X + \mathcal{N}$. We have that $\tilde{\varphi}$ is a valuation for \hat{F} . We let $\hat{\mathfrak{p}} = [\tilde{\varphi}]$. Also, we have a monomorphism $\mu : F \rightarrow \hat{F}$ by $x \mapsto [x]$ where $[x_n]$ stands for the equivalence class of $\{x_n\}$ in \hat{F} . We have that $\mu^*(\hat{\mathfrak{p}}) = \mathfrak{p}$ because

$$\tilde{\varphi}(\mu(x)) = \lim_{n \rightarrow \infty} \varphi(x) = \varphi(x)$$

Now consider $[X] \in \hat{F}$ with $X = \{x_n\} \in \mathcal{R}$. For each n , $[X] - \mu(x_n)$ is represented by the sequence

$$\{x_1 - x_n, x_2 - x_n, \dots\}$$

Then by using the property above,

$$\lim_{n \rightarrow \infty} \tilde{\varphi}([X] - \mu(x_n)) = \lim_{n \rightarrow \infty} \left(\lim_{m \rightarrow \infty} \varphi(x_m - x_n) \right) = 0$$

as $\{x_n\}$ is a Cauchy sequence. This shows that $\mu(F)$ is dense in \hat{F} . We have found an element in F that is arbitrary close to a point in \hat{F} .

Finally consider a Cauchy sequence $\{[X]_n\}$ of \hat{F} , then by density, there exists $y_n \in F$ such that

$$\tilde{\varphi}([X]_n - \mu(y_n)) < 1/n$$

for each n , then we have $\{[X]_n - \mu(y_n)\}$ is a null sequence which shows that $\{\mu(y_n)\}$ is a Cauchy sequence in \hat{F} . Then because $\tilde{\varphi}^\mu = \varphi$, we have that $\{y_n\}$ is a Cauchy sequence in F . Let $[Y] \in \hat{F}$ with $Y = \{y_n\}$, then we have

$$\tilde{\varphi}([Y] - \mu(y_n)) = 0 \Rightarrow \tilde{\varphi}([Y] - [X]_n) = 0$$

hence \hat{F} is $\hat{\mathfrak{p}}$ complete. The uniqueness is due to the following more general proposition, \square

Proposition 5.2. *Consider K, F be two fields with prime divisors \mathfrak{q} and \mathfrak{p} respectively. Suppose there exists a field embedding $\sigma : F \rightarrow K$ such that $\sigma^*(\mathfrak{q}) = \mathfrak{p}$. Let $(\hat{F}, \hat{\mathfrak{p}}, \mu)$ and $(\hat{K}, \hat{\mathfrak{q}}, \lambda)$ be $\mathfrak{p}, \mathfrak{q}$ completion of F, K respectively, then there exists a unique monomorphism $\hat{\sigma} : \hat{F} \rightarrow \hat{K}$ such that*

$$i) \ (\hat{\sigma})^*(\hat{\mathfrak{q}}) = \hat{\mathfrak{p}},$$

$$\begin{array}{ccc} \hat{F} & \xrightarrow{\hat{\sigma}} & \hat{K} \\ \mu \uparrow & & \uparrow \lambda \\ F & \xrightarrow{\sigma} & K \end{array}$$

$$ii) \ \hat{\sigma} \circ \mu = \mu' \circ \sigma,$$

Proof. Let $x \in \widehat{F}$. By denseness of F , there exists a Cauchy sequence $\{x_n\}$ in F such that $\mu(x_n) \rightarrow x$ in \widehat{F} . By assumption we have $\mu^*(\widehat{\mathfrak{p}}) = \mathfrak{p}$, $\sigma^*(\mathfrak{q}) = \mathfrak{p}$, $\lambda^*(\widehat{\mathfrak{q}}) = \mathfrak{q}$.

$$\{x_n\} \text{ Cauchy in } T_{\mathfrak{p}} \Leftrightarrow \{\sigma(x_n)\} \text{ Cauchy in } T_{\mathfrak{q}} \Leftrightarrow \{\lambda(\sigma(x_n))\} \text{ Cauchy in } T_{\widehat{\mathfrak{q}}}$$

as \widehat{K} is complete, we not define $\widehat{\sigma}$ by

$$\widehat{\sigma}(x) = \lim_{n \rightarrow \infty} \lambda(\sigma(x_n))$$

- i) Suppose $\{y_n\}$ is another Cauchy sequence that converges to x . We have that $\{x_n - y_n\}$ is a null sequence in $T_{\mathfrak{p}}$, then $\{\lambda(\sigma(x_n - y_n))\}$ is a null sequence in $T_{\widehat{\mathfrak{q}}}$. Hence

$$\lim_{n \rightarrow \infty} \lambda(\sigma(x_n)) = \lim_{n \rightarrow \infty} \lambda(\sigma(y_n))$$

- ii) We have that $\sigma, \lambda, \lim_{n \rightarrow \infty}$ has the additive, multiplicative property, hence $\widehat{\sigma}$ is a homomorphism,
iii)

$$\widehat{\sigma}\mu(x) = \lim_{n \rightarrow \infty} \lambda(\sigma(x)) = \lambda(\sigma(x))$$

shows that the diagram commutes.

- iv) Let $\widehat{\sigma}(x) = \widehat{\sigma}(y)$, then we have $\lim_{n \rightarrow \infty} \lambda(\sigma(x_n)) = \lim_{n \rightarrow \infty} \lambda(\sigma(y_n)) \Rightarrow x_n - y_n$ is a null sequence in F , hence $\lim_{n \rightarrow \infty} \mu(x_n - y_n) = 0 \Rightarrow x = \lim_{n \rightarrow \infty} \mu(x_n) = \lim_{n \rightarrow \infty} \mu(y_n) = y$.

Next step is to prove that $(\widehat{\sigma})^*(\widehat{\mathfrak{q}}) = \widehat{\mathfrak{p}}$. Let $\varphi \in \widehat{\mathfrak{q}}$, then we use that notation φ^λ for $\varphi \circ \lambda$, then $\varphi^{\lambda\sigma} \in \sigma^*(\lambda^*(\widehat{\mathfrak{q}})) = \sigma^*(\mathfrak{q}) = \mathfrak{p}$. As $\mu^*(\widehat{\mathfrak{p}}) = \mathfrak{p}$, there exists $\theta \in \widehat{p}$ such that $\theta^\mu = \varphi^{\lambda\sigma}$. Now let $x \in F$, then we have that

$$x = \lim_{n \rightarrow \infty} \mu(x_n)$$

$$\begin{aligned} \varphi^{\widehat{\sigma}}(x) &= \varphi(\widehat{\sigma}(x)) \\ &= \varphi\left(\lim_{n \rightarrow \infty} \lambda(\sigma(x_n))\right) \\ &= \lim_{n \rightarrow \infty} \varphi^{\lambda\sigma}(x_n) \\ &= \lim_{n \rightarrow \infty} \theta^\mu(x_n) \\ &= \theta\left(\lim_{n \rightarrow \infty} \mu(x_n)\right) = \theta(x) \end{aligned}$$

hence we have proved that $\varphi^{\widehat{\sigma}} \in \widehat{\mathfrak{p}}$. In particular, $(\widehat{\sigma})^*(\widehat{\mathfrak{q}}) = \widehat{\mathfrak{p}}$.

As we have proved existence, we are left to show uniqueness. Let $\widehat{\sigma}_1, \widehat{\sigma}_2$ be two extensions of σ with the desired properties, then $\widehat{\sigma}_1(\mu(F)) = \widehat{\sigma}_2(\mu(F))$ with $\mu(F)$ dense in \widehat{F} . Because a continuous mapping agrees in a dense set, and \widehat{K} is Hausdorff, we conclude that $\widehat{\sigma}_1 = \widehat{\sigma}_2$. \square

Let every exponential valuation of v of K , we have a completion K_v which extends canonically to a exponential valuation of K_v denoted again by v . There exists a unique extension \overline{v} to $\overline{K_v}$, the algebraic closure of K_v . The unique extension exists due to the following theorem.

Theorem 5.3. *Let F be complete with respect to the valuation φ . If K/F is an algebraic extension, φ is extended to a unique extension of φ to a valuation of L . If $[K : F] < \infty$, then the extension is given by*

$$\varphi'(x) = \sqrt[n]{\varphi(N_F^K(x))}$$

and L is complete respect to the extension.

Proof. We start with $[K : F] < \infty$. Clearly $N_F^K(x) = x^n$ for $x \in F$, hence $\varphi'|_K = \varphi$. Because $\varphi(y) \geq 0$, $\varphi'(x) \geq 0$, and $\sqrt[n]{x} = 0, \varphi(x) = 0, N_F^K(x) = 0 \Leftrightarrow x = 0$ shows that $\varphi'(x) = 0 \Leftrightarrow x = 0$. Also all three functions, $\sqrt[n]{}, \varphi, N_F^K$ are all multiplicative implies that φ' multiplicative. So it remains to show that $\varphi'(x) \leq 1 \Rightarrow \varphi'(1+x) \leq 1$.

Obviously, $\varphi'(x) \leq 1 \Rightarrow \sqrt[n]{\varphi(N_F^K(x))} \leq 1 \Rightarrow \varphi(N_F^K(x)) \leq 1$. Let $f = m_F(x)(t)$ be the minimal polynomial of x over F with $f = t^r + \cdots + a_0$. Then $N_F^K(x) = \pm a_0^d$ where $d = [K : F(x)]$ by A.3. This gives that $\varphi(a_r)^d \leq 1 \Rightarrow a_r \in \mathcal{O} \Rightarrow f \in \mathcal{O}[t]$ by 7.2. We now put $g(t) = f(t-1)$, then $g(1+x) = f(x) = 0$ with g minimal polynomial of $1+x$ over F .

$N_F^K(1+x) = (\pm g(0))^d = (\pm f(-1))^d = \pm((-1)^d + \cdots + a_r) \in \mathcal{O} \Rightarrow \varphi(N_F^K(1+x)) \leq 1$
 $\varphi'(1+x) \leq 1$ then easily follows.

If K/F is infinite, then we observe that

$$K = \bigcup_E E$$

where E runs over all finite intermediate field of K/F . For each E , there exists an extension φ_E of E . Let $x \in K$, then $x \in E$ for some E . We define $\varphi'(x) = \varphi_E(x)$. To finish the proof we need uniqueness which is dealt in a more general setting. \square

An finite dimensional F -vector space X is said to be **normed** over (F, φ) if there exists a norm function $\|\cdot\| : X \rightarrow \mathbb{R}$, satisfying,

- i) $\|\zeta\| \geq 0$ and $\|\zeta\| = 0 \Leftrightarrow \zeta = 0$,
- ii) $\|x\zeta\| = \varphi(x)\|\zeta\|$,
- iii) $\|\zeta + \eta\| \leq \|\zeta\| + \|\eta\|$.

Let (E, φ') be a extension of (F, φ) , then the additive group E with $\|\cdot\| = \varphi'$ is normed over (F, φ) . Also, if X is a finite dimensional vector space over F with w_1, \dots, w_n as its basis, then for all $\zeta \in X$, $\zeta = a_1 w_1 + \cdots + a_n w_n$. Define

$$\|\zeta\| = \max(\varphi(a_i))$$

which runs over all i , then $\|\cdot\|$ becomes a norm of X and call it the **canonical norm**.

Theorem 5.4. *Let F be complete respect with \mathfrak{p} and let $\varphi \in \mathfrak{p}$ with $\|\varphi\| \leq 2$. Suppose that X is a finite dimensional vector space over F , and $|\cdot|$ be any norm on X over (F, φ) , then X is complete topological group in the metric topology determined by $|\cdot|$ and there exists $C_1, C_2 > 0$ such that*

$$C_1 \|\zeta\| \leq |\zeta| \leq C_2 \|\zeta\|$$

for all $\zeta \in X$.

Proof. Let $\{\zeta_m\}$ be Cauchy sequence respect to $|\cdot|$, then for all $\varepsilon \in \mathbb{R}^{>0}$, we have

$$\|\zeta_{m_1} - \zeta_{m_2}\| < \varepsilon \text{ whenever } m_1, m_2 \geq N$$

with $\zeta_m = a_{m,1}w_1 + \cdots + a_{m,n}w_n$. We then have a natural inequality,

$$\varphi(z_{m_1,i} - z_{m_2,i}) \leq \|z_{m_1} - z_{m_2}\| < \varepsilon$$

shows that each component is a Cauchy sequence in F , thus there exists a_j such that $a_{m,j} \rightarrow a_j$. Let $\zeta = a_1w_1 + \cdots + a_nw_n$, then we claim that $\zeta_m \rightarrow \zeta$. For any ε , and for all i , there exists N_i such that

$$m \geq N_i \Rightarrow \varphi(a_{m,i} - a_i) < \varepsilon$$

then if $N = \max(N_i)$, implies that

$$m \geq N \Rightarrow \|\zeta_m - \zeta\| = \max(\varphi(a_{m,i} - a_i)) < \varepsilon$$

which proves the claim. Furthermore, proves that X is complete with respect to $\|\cdot\|$.

Let $\zeta = a_1w_1 + \cdots + a_nw_n$, then

$$\begin{aligned} |\zeta| &= |a_1w_1 + \cdots + a_nw_n| \\ &\leq |a_1w_1| + \cdots + |a_nw_n| \\ &= \varphi(a_1)|w_1| + \cdots + \varphi(a_n)|w_n| \\ &\leq \|\zeta\||w_1| + \cdots + \|\zeta\||w_n| = C_2\|\zeta\| \end{aligned}$$

if we let $C_2 = |w_1| + \cdots + |w_n|$. If $n = 1$, then $\varphi = |\cdot|$, hence the result is immediate. Suppose that we have the conclusion for $n - 1$ -dimensional. Then we define

$$Y_i = Fw_1 + \cdots + Fw_{i-1} + Fw_{i+1} + \cdots + Fw_n$$

then $X = Y_i + Fw_i$. We have that Y_i is complete by induction hypothesis. Y_i complete implies that Y_i closed in X as all limit point of Y_i has a Cauchy sequence in Y_i . Since X is a topological group, $Y_i + w_i$ is closed. Because $0 \notin Y_i + w_i$, so $0 \notin \cup_{i=1}^n (Y_i + w_i)$ which is also closed. There exists a neighborhood of 0 disjoint from the union. Hence there exist C_1 such that

$$|\eta_i + w_i| \geq C_1$$

for all $\eta_i \in Y_i$. If $\zeta = a_1w_1 + \cdots + a_nw_n$ nonzero with $\varphi(a_r)\|\zeta\|$, then $a_r \neq 0$, and

$$|a_r^{-1}| = |(a_1/a_r)w_1 + \cdots + w_r + \cdots + (a_n/a_r)w_n| \geq C_1$$

hence we have that $|\zeta| \geq C_1\varphi(a_r) = C_1\|\zeta\|$.

For all $y \in B_{|\cdot|}(x, \varepsilon)$, $y \in B_{\|\cdot\|}(x, \varepsilon/C_1) \subset B_{|\cdot|}(x, \varepsilon)$, and similar process shows that the topology induced by both norms are equivalent. \square

Proposition 5.5. *Let F be \mathfrak{p} -complete and K/F be finite. If an extension of \mathfrak{p} exists, then it is unique. Furthermore, if K/F be algebraic extension, then the extension of \mathfrak{p} is unique if it exists.*

Proof. First for the finite case, we choose $\varphi \in \mathfrak{p}$ such that $\|\varphi\| \leq 2$, with φ_1, φ_2 be two extensions of φ to K . Then by above, $\varphi_1 = \varphi_2^\alpha$ because they induce the same topology. Furthermore, $\varphi_1|_F = (\varphi_2|_F)^\alpha \Rightarrow \varphi = \varphi^\alpha \Rightarrow \alpha = 1$. We thus see that they are equal.

Now for algebraic extension K/F , let φ_1, φ_2 be two distinct extensions of φ to K , then there exists $x \in K$ such that $\varphi_1(x) \neq \varphi_2(x)$, but φ_1 and φ_2 coincide in $F(x)$. Hence leads to contradiction. \square

Let K/F be finite with $\varphi \in \mathfrak{p}$ be valuation of F and $\psi \in \mathfrak{q}$ be valuation of K extending φ . Also, we have the canonical extension $\tilde{\varphi}$ of φ to $F_{\mathfrak{p}}$. We also have unique extension $\bar{\varphi}$ of $\tilde{\varphi}$ to $\bar{F}_{\mathfrak{p}}$.

We first show that $F_{\mathfrak{p}} \subset K_{\mathfrak{q}}$. If we denote $[x_n]_{\mathfrak{p}} \in F_{\mathfrak{p}}$ for the \mathfrak{p} -Cauchy sequence with $x_n \in F$. Similarly, $[x_n]_{\mathfrak{q}}$ denote \mathfrak{q} -Cauchy sequence with $x_n \in K$. As $F \subset K$, we consider the map $[x_n]_{\mathfrak{p}} \mapsto [x_n]_{\mathfrak{q}}$. For $x_n, y_n \in F$,

$$[x_n]_{\mathfrak{p}} = [y_n]_{\mathfrak{p}} \Leftrightarrow \lim_{n \rightarrow \infty} \varphi(x_n - y_n) = 0 \Leftrightarrow \lim_{n \rightarrow \infty} \psi(x_n - y_n) = 0 \Leftrightarrow [x_n]_{\mathfrak{q}} = [y_n]_{\mathfrak{q}}$$

show that the map is well-defined and injective. Hence we proved the inclusion of $F_{\mathfrak{p}}$ into $K_{\mathfrak{q}}$.

$F_{\mathfrak{p}}/F$ and K/F finite implies that $KF_{\mathfrak{p}}/F_{\mathfrak{p}}$ is finite. As K and $F_{\mathfrak{p}}$ both lies inside $K_{\mathfrak{q}}$, we have $KF_{\mathfrak{p}} \subset K_{\mathfrak{q}}$. If $\tilde{\psi}$ denote the canonical extension of ψ , then we give $KF_{\mathfrak{p}}$ the valuation $\tilde{\psi}|_{KF_{\mathfrak{p}}}$, then since it extends ψ , we see that it must be uniquely determined and $KF_{\mathfrak{p}}$ is complete. Observing the tower of fields,

$$K \subset KF_{\mathfrak{p}} \subset K_{\mathfrak{q}}$$

we see that every completing via \mathfrak{q} , we get

$$K_{\mathfrak{q}} \subset KF_{\mathfrak{p}} \subset K_{\mathfrak{q}} \Rightarrow K_{\mathfrak{q}} = KF_{\mathfrak{p}}$$

Hence $K_{\mathfrak{q}}/F_{\mathfrak{p}}$ is a finite extension. We are now ready to prove the extension theorem which is the following

Theorem 5.6 (Extension Theorem). *Let K/F be a finite extension and $\varphi \in \mathfrak{p}$ be a valuation of F , then every extension ψ of φ arises as the composite $\psi = \bar{\varphi} \circ \tau$ for some embedding $\tau : K \rightarrow \bar{F}_{\mathfrak{p}}$.*

Proof. With the above notation, $K_{\mathfrak{q}} \subset \bar{F}_{\mathfrak{p}}$ shows that $\bar{\varphi}|_{K_{\mathfrak{q}}} = \tilde{\psi}$ as $\tilde{\psi}$ is the unique extension of $\tilde{\varphi}$. Because $K_{\mathfrak{q}}/F_{\mathfrak{p}}$ finite, we have a $F_{\mathfrak{p}}$ -embedding,

$$\tau : K_{\mathfrak{q}} \rightarrow \bar{F}_{\mathfrak{p}}$$

Clearly, $\varphi \circ \tau$ is a valuation of $K_{\mathfrak{q}}$, and $(\bar{\varphi} \circ \tau)|_{F_{\mathfrak{p}}} = \bar{\varphi} \circ \tau|_{F_{\mathfrak{p}}} = \bar{\varphi}|_{F_{\mathfrak{p}}} = \tilde{\varphi}$. We have a F -embedding, $\tau|_{\mathfrak{p}} : K \rightarrow \bar{F}_{\mathfrak{p}}$,

$$\tilde{\varphi} = \bar{\varphi} \circ \tau|_{F_{\mathfrak{p}}}$$

□

Before we classify the archimedean valuations of a number field k , we state the theorem due to Ostrowski.

Theorem 5.7 (Ostrowski). *Let K be complete respect to an archimedean valuation $|\cdot|$, then there exists an isomorphism σ of K to either \mathbb{R} or \mathbb{C} . If \mathfrak{p}_{∞} denotes the prime divisor of $|\cdot|$ and \mathfrak{q}_{∞} denotes the prime divisor of the usual absolute value of either \mathbb{R} or \mathbb{C} , then $\sigma^*(\mathfrak{q}_{\infty}) = \mathfrak{p}_{\infty}$.*

Proof. K having archimedean valuation implies that K has characteristic 0, the prime field of K is isomorphic to \mathbb{Q} . By 5.2, we may assume that $\mathbb{R} \subset K$. Next we prove that K is algebraic over \mathbb{R} , then K is embedded in \mathbb{C} , hence $K = \mathbb{R}$ or $K = \mathbb{C}$.

So consider $\zeta \in K$ and a continuous map $f : \mathbb{C} \rightarrow \mathbb{R}$ defined by

$$f(z) = |\zeta^2 - (z + \bar{z})\zeta + z\bar{z}|$$

with $z + \bar{z}, z\bar{z} \in \mathbb{R}$. We first observe that $\lim_{z \rightarrow \infty} f(z) = \infty$. If we let $\zeta = a + bi$, then

$$f(z) = |(a + bi)^2 - 2\operatorname{Re}(z)(a + bi) + \operatorname{Re}(z)^2 + \operatorname{Im}(z)^2|$$

then $\operatorname{Im}(z) \rightarrow \infty$ easily shows that $f(z) \rightarrow \infty$.

Let z_0 be any complex number, then let $M = f(z_0)$, then there exists N such that $|z| > N \Rightarrow |f(z)| > M$. There exists $z_m \in \mathbb{C}$ such that $f(z_m)$ is minimal in $f(\overline{B(0, N)})$ as $\overline{B(0, N)}$ is compact. Hence there exists a minimum value for f . We let $f(z_m) = m$. Because $\{m\}$ is closed in \mathbb{R} , we have

$$S = \{z \in \mathbb{C} \mid f(z) = m\}$$

is nonempty, bounded, and closed as f is continuous. Also because S is closed, there exists z_0 such that $|z_0| \geq |z|$ for all $z \in S$, i.e. the supremum. It suffices to show that $m = 0$, then ζ is algebraic over \mathbb{R} .

Suppose for contradiction that $m > 0$, then there exists $0 < \varepsilon < m$ and a polynomial in real coefficients

$$g(x) = x^2 - (z_0 + \bar{z}_0)x + z_0\bar{z}_0 + \varepsilon$$

with roots $z_1, \bar{z}_1 \in \mathbb{C}$. If $z_0 \in \mathbb{R}$, then we have

$$g(x) = x^2 + z_0^2 + \varepsilon \Rightarrow z_1 = \sqrt{z_0^2 + \varepsilon}$$

If $z_0 \in \mathbb{C} \setminus \mathbb{R}$, then we have that $\operatorname{Re}(z_0) = \operatorname{Im}(z_1)$. Let's denote it a . $z_0 = a + bi$ and $z_1 = a + ci$. Then we have $a^2 + c^2 = a^2 + b^2 + \varepsilon \Rightarrow c = \sqrt{b^2 + \varepsilon}$.

Because

$$z_0\bar{z}_0 + \varepsilon = z_1\bar{z}_1 \Rightarrow |z_1| > |z_0| \Rightarrow f(z_1) > m$$

Let $n \in \mathbb{N}$ be fixed and consider another real polynomial

$$G(x) = [g(x) - \varepsilon]^n - (-\varepsilon)^n = \prod_{i=1}^{2n} (x - \alpha_i) = \prod_{i=1}^{2n} (x - \bar{\alpha}_i)$$

then clearly $G(z_1) = 0$, so we may assume that $z_1 = \alpha_1$ without loss of generosity. Now we substitute ζ , then we get

$$|G(\zeta)|^2 = \prod_{i=1}^{2n} f(\alpha_i) \geq f(\alpha_1)m^{2n-1}$$

Furthermore,

$$|G(\zeta)| \leq |g(\zeta) - \varepsilon|^n + |-\varepsilon|^n = |\zeta^2 - (z_0 + \bar{z}_0)\zeta + z_0\bar{z}_0|^n + \varepsilon^n = f(z_0)^n + \varepsilon^n = m^n + \varepsilon^n$$

then

$$f(\alpha_1)m^{2n-1} \leq (m^n + \varepsilon^n)^2$$

$$\frac{f(\alpha_1)}{m} \leq \left(1 + \left(\frac{\varepsilon}{m}\right)^n\right)$$

then as $n \rightarrow \infty$, we get $f(\alpha_1) \leq m$, which contradicts our assumption. \square

Proposition 5.8. *Let φ be an archimedean valuation of \mathbb{Q} , then there exists $\alpha \in \mathbb{R}^{\geq 0}$ such that for all $x \in \mathbb{Q}$,*

$$\varphi(x) = |x|^\alpha$$

where $| \cdot |$ the usual absolute value of \mathbb{Q} .

Proof. Let $m, n \in \mathbb{Z}$ both greater than 1. For any integer $t > 0$, we can write

$$m^t = a_0 + a_1 n + \cdots + a_s n^s$$

where $a_i \in \mathbb{Z}$ and $0 \leq a_i < n$ with $a_s \neq 0$. Because $a_s \geq 1$, we have that $n^s \leq m^t$, which taking the log gives $s \log n \leq t \log m$. We thus have

$$s \leq t \frac{\log m}{\log n}$$

Also we have that $\varphi(n) \leq \varphi(1) + \cdots + \varphi(1) = n$ for any n , so we get

$$\varphi(a_i) \leq a_i < n$$

It follows that

$$\begin{aligned} \varphi(m^t) &\leq \varphi(a_0) + \cdots + \varphi(a_s) \varphi(n)^s \\ &\leq n(1 + \cdots + \varphi(n)^s) \\ &\leq n(s+1)M^s \text{ where } M = \max(1, \varphi(n)) \\ &\leq n \left(1 + t \frac{\log m}{\log n}\right) [\max(1, \varphi(n))]^{t(\log m / \log n)} \end{aligned}$$

Take the t^{th} root of unity, we get

$$\varphi(m) \leq \max(1, \varphi(n))^{(\log m / \log n)}$$

Now we assert that $\varphi(n) > 1$ for $n > 1$ because if there exists $n_0 > 1$ with $\varphi(n_0) \leq 1$, then we get

$$\varphi(m) \leq 1 \text{ for all } m \in \mathbb{Z}$$

which contradicts 4.1 which says that archimedean valuation has $\{\varphi(m) \mid m \in \mathbb{Z}\}$ unbounded. Hence we achieve a relationship

$$\varphi(m) \leq \varphi(n)^{\log n / \log m} \Rightarrow \varphi(m)^{1/\log m} \leq \varphi(n)^{1/\log n}$$

Because m, n were arbitrary, we get the equality

$$\varphi(m)^{1/\log m} = \varphi(n)^{1/\log n} = e^\alpha$$

for some $\alpha \in \mathbb{R}^{>0}$ because $\varphi(m) > 1 \Rightarrow \varphi(m)^{1/\log m} > 1$. Hence we get

$$\varphi(n) = e^{\alpha \log n} = n^\alpha$$

for any $n > 1$, so for any $n \in \mathbb{Z}$, $\varphi(n) = |n|^\alpha$. By multiplicative property of $|\cdot|$, we conclude that $\varphi(x) = |x|^\alpha$ for all $x \in \mathbb{Q}$. \square

Let k be a number field and φ be an archimedean valuation, then we have that φ is an extension of $|\cdot|$, the absolute value of \mathbb{Q} . Because k/\mathbb{Q} is an algebraic extension, by the existence theorem, all archimedean valuations arise from $\sigma : k \rightarrow \mathbb{C}$ as $\mathbb{C} = \overline{\mathbb{Q}}_|\cdot|$, i.e. classified by the complex embeddings of k , $\text{Hom}(k, \mathbb{C})$. We have

$$\text{Hom}(k, \mathbb{C}) := \{\sigma_1, \dots, \sigma_n\}$$

where $\sigma_1, \dots, \sigma_r$ is the real embeddings of k and $\sigma_{r+1}, \overline{\sigma_{r+1}}, \dots, \sigma_{r+s}, \overline{\sigma_{r+s}}$ which are complex embeddings of k . Thus we have $r + 2s = n$. Because $|\sigma(x)| = \sigma(x) \overline{\sigma(x)} = |\overline{\sigma(x)}|$, we have σ_i and $\overline{\sigma_i}$ induces the same topology. Now consider the following set of valuations M_k

$$\sigma_1, \dots, \sigma_{r+s}, v_{\mathfrak{p}}$$

where $v_{\mathfrak{p}}$ is the normalized discrete nonarchimedean valuations of k with \mathfrak{p} varies over all prime ideals of k . M_k is called the **canonical set** of k . We will use $v \in M_k$

to mean both the archimedean and nonarchimedean valuations of k to unify the notation.

Proposition 5.9. *Let $v_1, v_2 \in M_k$, then v_1 and v_2 are not equivalent.*

Proof. We will prove later in 8.3 that for any two distinct v_i with its corresponding valuation φ_i , there exists $x \in k$ such that

$$\varphi_1(x) > 1 \text{ and } \varphi_2(x) < 1 \quad (\dagger)$$

Because the set $B(0, 1)$ consists of $x \in k$ such that $x^n \rightarrow 0$ as $n \rightarrow \infty$, $B(0, 1)$ is determined the topology. (\dagger) clearly shows that $B(0, 1)$ is distinct elements in the canonical set, hence v_1 and v_2 are not equivalent. This easily extends to the fact that k_{v_1} and k_{v_2} are not isomorphic as their $B(0, 1)$ are different when restricted to k . \square

We conclude this section by observing that M_k is, in fact, a system of representatives of all prime divisors of k , hence the name canonical set of k .

6. TOPOLOGY ON LOCAL FIELDS

Let \mathcal{O} be a Dedekind domain with \mathfrak{p} be a prime ideal. $\mathcal{O}_{\mathfrak{p}}$, the localization of \mathcal{O} at \mathfrak{p} is a discrete valuation ring. We have (π) is the unique maximal ideal of $\mathcal{O}_{\mathfrak{p}}$. We define

$$A_n := \mathcal{O}_{\mathfrak{p}}/(\pi)^n$$

which gives a inverse system with canonical epimorphisms. We let

$$\mathcal{O}_v^a := \varprojlim_m A_m$$

where the superscript a refers to its algebraic construction. Because for any m , we have an isomorphism

$$\mathcal{O}/\mathfrak{p}^m \cong \mathcal{O}_{\mathfrak{p}}/(\pi)^m$$

we get $\mathcal{O}_v^a = \varprojlim_m \mathcal{O}/\mathfrak{p}^m$ which is analogous to the construction of p -adic numbers from integers. By the definition of the inverse limit, the elements in \mathcal{O}_v^a is of the form (x_i) where $\pi_m(x_m) = x_{m-1}$ with $\pi_m : A_m \rightarrow A_{m-1}$ the canonical epimorphism.

If $|\mathcal{O}_k/\mathfrak{p}| = p^f$ with $(p) = \mathfrak{p} \cap \mathbb{Z}$, then we can choose a system of representatives of a_0, \dots, a_{p^f-1} with 0 included, then for any $(x_i) \in \mathcal{O}_v^a$,

$$x_1 \equiv c_0 \pmod{\pi}$$

So we consider $x_1 - c_0 = (x_i - c_0)$, then because $x_1 - c_0$ is divisible by π , the first coordinate is 0, then because we have the commutative diagram

$$\begin{array}{ccc} \mathcal{O}_{\mathfrak{p}} & & \\ \pi_n \downarrow & \searrow \pi_m & \\ \mathcal{O}_{\mathfrak{p}}/(\pi)^n & \xrightarrow{\pi_m^n} & \mathcal{O}_{\mathfrak{p}}/(\pi)^m \end{array}$$

with $\pi_m^n : \mathcal{O}_{\mathfrak{p}}/(\pi)^n \rightarrow \mathcal{O}_{\mathfrak{p}}/(\pi)^m$ a canonical epimorphism. We see that all $x_i - c_0$ are divisible by π , hence

$$\begin{aligned} x - c_0 &= (x_i - c_0) \\ &= (\pi x'_i) \\ &= \pi(x'_i) \end{aligned}$$

we may continue the process and realize that

$$\begin{aligned} x &= c_0 + (x - c_0) \\ &= c_0 + (\pi x') \\ &= c_0 + \pi(c_1 - (x' - c_1)) \\ &= c_0 + c_1\pi + c_2\pi^2 + \cdots \end{aligned}$$

where c_i are chosen from the system of representatives. Hence we clearly get that all elements in \mathcal{O}_v^a can be uniquely expressed as a infinite sum of the form

$$\sum_{n=0}^{\infty} c_n \pi^n$$

which correspond to $x = (x_i)$ with $x_i = \sum_{n=0}^i c_n \pi^n$.

Now we will construct *the ring of integers* \mathcal{O}_v topologically when v is a nonarchimedean valuation. We may define the following invariants

- i) $\mathcal{O}_v = \{x \in k_v \mid v(x) \geq 0\} = \{x \in k_v \mid \varphi_v(x) \leq 1\}$, the **valuation ring** of k_v .
- ii) $\mathfrak{p}_v = \{x \in k_v \mid v(x) > 0\} = \{x \in k_v \mid \varphi_v(x) < 1\}$, the **maximal ideal** of \mathcal{O}_v
- iii) $U_v = \{x \in k_v \mid v(x) = 0\} = \{x \in k_v \mid \varphi_v(x) = 1\}$, the **unit group** of \mathcal{O}_v .

We observe that v is discrete as v is nonarchimedean exponential valuation of a number field, hence \mathcal{O}_v is a discrete valuation ring with some fixed prime number $\pi \in \mathcal{O}_v$.

Proposition 6.1. *We have the isomorphism*

$$\mathcal{O}_v/\mathfrak{p}_v^n \cong \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{\mathfrak{p}}^n$$

In particular, $\mathcal{O}_v/\mathfrak{p}_v$ is finite.

Proof. We first need to show that \mathcal{O}_v is the closure of $\mathcal{O}_{\mathfrak{p}}$. For any Cauchy sequence $\{x_n\}$ of \mathcal{O}_v that converges to x , we have that $\varphi_{\mathfrak{p}}(x_n) \leq 1 \Rightarrow \varphi_{\mathfrak{p}}(x) \leq 1 \Rightarrow x \in \mathcal{O}_v$, hence \mathcal{O}_v is closed. Now let $x \in \mathcal{O}_v \setminus \mathcal{O}_{\mathfrak{p}}$. We have $x = \lim_{n \rightarrow \infty} x_n$ for $x_n \in k$. Because $\varphi_{\mathfrak{p}}$ is discrete, we have that there exists n_0 such that $n \geq n_0 \Rightarrow \varphi_{\mathfrak{p}}(x) = \varphi_{\mathfrak{p}}(x_n) \leq 1$. This is same as saying that $x_n = a_n/b_n$ for some $a_n, b_n \in \mathcal{O}_k$ with $\varphi_{\mathfrak{p}}(b_n) = 1$. Because we know that $\mathfrak{p} = (\pi)$ for some prime element, we can always find y_n such that

$$b_n y_n \equiv a_n \pmod{\pi^n}$$

Then We have $\varphi_{\mathfrak{p}}(x_n - y_n) \leq \frac{1}{(p^f)^n}$. $x = \lim_{n \rightarrow \infty} y_n$, hence $x \in \overline{\mathcal{O}_{\mathfrak{p}}}$, the closure of $\mathcal{O}_{\mathfrak{p}}$.

Combining the two, we see that \mathcal{O}_v is a closure of $\mathcal{O}_{\mathfrak{p}}$.

Now consider the map

$$a \mapsto a \pmod{\mathfrak{p}_v^n} \text{ defined for } \mathcal{O}_{\mathfrak{p}} \rightarrow \mathcal{O}_v/\mathfrak{p}_v^n$$

The same prime element in $\mathcal{O}_{\mathfrak{p}}$ is also a prime element for \mathcal{O}_v as they are both discrete valuation ring. Thus the kernel is simply $\mathfrak{p}\mathcal{O}_{\mathfrak{p}}^n$, so we now show that the

map is surjective. Let $x \in \mathcal{O}_v$, then there exists $a \in \mathcal{O}_{\mathfrak{p}}$ such that

$$\varphi_{\mathfrak{p}}(x - a) \leq \frac{1}{(p^f)^n}$$

because it either lies inside $\mathcal{O}_{\mathfrak{p}}$ or is a limit point, then by definition $x - a \in \mathfrak{p}_v^n$, i.e. $x \cong a \pmod{\mathfrak{p}_v^n}$. The isomorphism has been established. \square

Hence we can choose a system of representative of $\mathcal{O}_v/\mathfrak{p}_v$ from \mathcal{O}_v containing 0 which will be denoted \mathcal{R} where $p^f = |\mathcal{O}_v/\mathfrak{p}_v|$ with $(p) = \mathfrak{p} \cap \mathbb{Z}$ and $f = [\mathcal{O}_k/\mathfrak{p} : \mathbb{Z}/(p)]$.

Theorem 6.2. *Every element x in k_v can be uniquely expressed into the form*

$$x = \sum_{i=m}^{\infty} a_i \pi^i$$

where $m \in \mathbb{Z}$ with $c_i \in \mathcal{R}$. Furthermore, every such infinite sum represents an element of k_v with $v(x) = m$.

Proof. Let $x = \pi^m u$ with $u \in \mathcal{O}_v^*$. Let $\mathcal{O}_v/\mathfrak{p}_v \cong \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$, then $\bar{u} \in \mathcal{O}_v/\mathfrak{p}_v$ has a unique nonzero representation $a_0 \in \mathcal{R}$. Hence we have $u = a_0 + \pi b_1$ for some $b_1 \in \mathcal{O}_v$. Assume $a_0, \dots, a_{n-1} \in \mathcal{R}$ satisfies

$$u = a_0 + \dots + a_{n-1} \pi^{n-1} + \pi^n b_n$$

with a_i uniquely determined by $b_n = a_n + \pi b_{n+1}$, then by the same process, we obtain

$$u = a_0 + \dots + a_n \pi^n + \pi^{n+1} b_{n+1}$$

Then we have uniquely determined $\sum_{i=m}^{\infty} a_i \pi^i$ by u , and this converges to u because $\pi^{n+1} b_{n+1}$ converges to 0. \square

We consider the open balls

$$B(0, p^{-fs})$$

where $s \in \mathbb{Z}$, then

$$y \in B(0, p^{-fs}) \Leftrightarrow v_{\mathfrak{p}}(y) > s \Leftrightarrow y = \sum_{n=s+1}^{\infty} c_n \pi^n$$

Hence we immediately see that

- i) $\mathcal{O}_v = B(0, p^f)$,
- ii) $\mathfrak{p}_v = B(0, 1)$,
- iii) $U_v = \mathcal{O}_v - \mathfrak{p}_v$.

by comparing the definition. Now for any fundamental open sets $B(0, \gamma)$, by discreteness, we have

$$B(0, \gamma) = \overline{B(0, \gamma - \varepsilon)}$$

for sufficiently small $\varepsilon > 0$. Hence all fundamental open sets are closed. It follows that $\mathcal{O}_v, \mathfrak{p}_v, U_v$ are all open and closed. In fact, for any fundamental open sets $B(x, p^{-fs})$ and $B(0, p^f)$ we have a homeomorphism

$$y \mapsto \pi^{-s-1}(y - x)$$

Theorem 6.3. *k_v is locally compact topological field with compact subsets \mathcal{O}_v and \mathcal{O}_v^* .*

Proof. The proof that k_v is a topological field coincides with the proof that \mathbb{R} is a topological space in 2.11. Let's consider

$$A_m := \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{\mathfrak{p}}^m$$

then we have that A_m is finite, hence compact, so by the Tychonoff theorem, we have that the product

$$\prod_{m=1}^{\infty} A_m$$

is compact. Let $(a_m) \notin \mathcal{O}_v$, then there exists m_0 such that $\varphi_{m_0}(a_{m_0}) \neq a_{m_0-1}$ with $\varphi_{m_0} : A_{m_0} \rightarrow A_{m_0-1}$, the canonical epimorphism. Now consider the set

$$\{a_0\} \times \cdots \times \{a_{m_0}\} \times \prod_{m>m_0} A_m$$

is open in the product topology, and is disjoint from \mathcal{O}_v since beginning of every element has $\varphi_{m_0}(a_{m_0}) \neq a_{m_0-1}$. This shows that \mathcal{O}_v^c is open, and thus \mathcal{O}_v closed. \mathcal{O}_v is a closed subset of $\prod A_m$, hence \mathcal{O}_v is compact. \mathcal{O}_v^* is a closed subset of \mathcal{O}_v , hence compact. \square

We conclude by saying that because any two fundamental open sets are homeomorphic, and fundamental open sets are open, closed, and compact simultaneously.

We have established in the previous section that there was a unique representation of the same form for \mathcal{O}_v , so we have established an algebraic isomorphism

$$\mathcal{O}_v \cong \mathcal{O}_v^a$$

We then define $v_{\mathfrak{p}}^a : \mathcal{O}_v^a \rightarrow \mathbb{Z} \cup \{\infty\}$ by $v_{\mathfrak{p}}^a(x) = m$, where m is the smallest such that c_m is nonzero. Under the isomorphism above, we see that $v_{\mathfrak{p}}^a$ induces an exponential valuation of \mathcal{O}_v . This coincide with normalized discrete valuation $v_{\mathfrak{p}}$.

For all $\mathcal{O}_{\mathfrak{p}}/(\pi)^n$, we give discrete topology and give the product

$$\prod \mathcal{O}_{\mathfrak{p}}/(\pi)^n$$

the product topology. Finally, one gives \mathcal{O}_v^a the subspace topology. We will continue to denote $\mathcal{O}_{\mathfrak{p}}/(\pi)^n = A_n$. Then the fundamental open sets in the product topology is of the form,

$$\prod_{n=1}^{\infty} B_n \cap \mathcal{O}_v^a$$

where $B_n \subset A_n$, and $B_n = A_n$ for almost all n . Then because of the finiteness the above set is of the form

$$U = \left(\prod_{n=1}^m B_n \times \prod_{n=m+1}^{\infty} A_n \right) \cap \mathcal{O}_v^a$$

then any $x \in U$, we have that $x \in B(x, p^{-fm}) \subset U$. In fact, if $y \in B(x, p^{-fm})$, then

$$y - x = \sum_{n=m+1}^{\infty} c_n \pi^n \Rightarrow y = x + \sum_{n=m+1}^{\infty} c_n \pi^n$$

then because $x \in U$ and the n -th coefficient where $n > m$ doesn't matter, so we have $y \in U$. This shows that the metric topology is finer.

Conversely, if $x \in k_v$ with

$$x = \sum_{n=1}^{\infty} c_n \pi^n$$

then we have that

$$B(x, p^{-fm}) = \prod_{n=1}^m \{c_n\} \times \prod_{n=m+1}^{\infty} A_n$$

hence we have that the metric topology and the topology induced by the inverse limit coincide. We have thus established an algebraic and topological isomorphism

$$\begin{aligned} \mathcal{O}_v &\cong \mathcal{O}_v^a \\ &= \varprojlim \mathcal{O}_{\mathfrak{p}}/(\pi)^n \\ &\cong \varprojlim \mathcal{O}_k/\mathfrak{p}^n \end{aligned}$$

7. HENSEL'S LEMMA

For a field F with a nonarchimedean prime divisor \mathfrak{p} , we denote \mathcal{O} or $\mathcal{O}_{v_{\mathfrak{p}}}$ to be its valuation ring and denote \mathfrak{p} to be the unique prime ideal of \mathcal{O} . $\kappa = \mathcal{O}/\mathfrak{p}$ will always denote the residue class field of F with respect to \mathfrak{p} .

Lemma 7.1 (Hensel's Lemma). *Let F be complete with respect to the nonarchimedean prime divisor \mathfrak{p} , and let $f \in \mathcal{O}[t]$ be primitive, i.e. $\bar{f} \neq 0$ in $\kappa[t]$. Suppose \bar{f} admits a factorization*

$$\bar{f} = GH \text{ in } \kappa[t]$$

with G, H relatively prime polynomials in $\kappa[t]$, then there exists $g, h \in \mathcal{O}[t]$ such that

- i) $f = gh$,
- ii) $\bar{g} = G, \bar{h} = H$,
- iii) $\deg(g) = \deg(G)$.

Proof. To simplify the notation, we will use the following convention $\deg(f) = d_f$. It is clear that $d_{\bar{f}} \leq d_f$ and $d_G + d_H = d_{\bar{f}} \leq d_f$, hence $d_G \leq d_f - d_G$. We let $g_1, h_1 \in \mathcal{O}[t]$ with $\bar{g}_1 = G$ and $\bar{h}_1 = H$, with $d_{g_1} = d_G$ and $d_{h_1} = d_H$. This can be easily done by observing that

$$G = \bar{a}_s t^s + \cdots + \bar{a}_0$$

can be represented by

$$g_1 = a_s t^s + \cdots + a_0$$

We may assume that G is monic because $\bar{f} = (\bar{a}_s^{-1}G)(\bar{a}_s H)$, so from now on, G and g_1 is monic. Because $(G, H) = 1$, there exists $\alpha, \beta \in \mathcal{O}[t]$ such that $\bar{\alpha}G + \bar{\beta}H = 1$. This equality and the modulo \mathfrak{p} factorization of \bar{f} show that $f - g_1 h_1, \alpha g_1 + \beta h_1 - 1 \in \mathfrak{p}[t]$, i.e. all coefficient of these polynomials are all nonzero. Let $v \in \mathfrak{p}$, then \bar{v} be the canonical extension of v to $F(t)$. We let

$$\varepsilon = \min(\bar{v}(f - g_1 h_1), \bar{v}(\alpha g_1 + \beta h_1 - 1))$$

If $\varepsilon = \infty$, then we have that $f - g_1 h_1$ has all of its coefficient 0, which gives the desired f and g , so we assume that $0 < \varepsilon < \infty$. Because there are only finite

number of coefficients, there exists $\pi \in \mathfrak{p}$, one of the coefficient, such that $v(\pi) = x$. For all $i \in \mathbb{N}$, we would like to find g_i, h_i such that

- i) $f \equiv g_i h_i \pmod{\pi^i}$,
- ii) $\overline{g_i} = G$ and $\overline{h_i} = H$,
- iii) $g_i \equiv g_{i-1} \pmod{\pi^{i-1}}$, $h_i \equiv h_{i-1} \pmod{\pi^{i-1}}$ for $i \geq 2$,
- iv) $d_{g_i} = d_G$ and $d_{h_i} \leq d_f - d_G$.

Let c_i denote the coefficient of $f - g_1 h_1$, then $v(c_i) \geq v(\pi) \Rightarrow v(c_i/\pi) = v(c_i) - v(\pi) \geq 0$. This shows that there exists $d_i \in \mathcal{O}$ such that $c_i = \pi d_i \Rightarrow f - g_1 h_1 \in \pi \mathcal{O}[t]$, hence i) is satisfied. ii) and iv) is satisfied by construction. Now suppose that we have established the result for $n-1$ with $n \geq 2$ and also that we have found

$$\begin{aligned} g_n &= g_{n-1} + \pi^{n-1}u \\ h_n &= h_{n-1} + \pi^{n-1}v \end{aligned}$$

for some $u, v \in \mathcal{O}[t]$, then it is clear that iii) is satisfied. Notice that we have not used the induction hypothesis of iii), so the construction can be used for $i = 2$. Also because $\pi \in \mathfrak{p}$, it is clear that

$$\overline{g_n} = \overline{g_{n-1}} + \overline{\pi^{n-1}u} = \overline{g_{n-1}} = G \text{ and } \overline{h_n} = \overline{h_{n-1}} + \overline{\pi^{n-1}v} = \overline{h_{n-1}} = H$$

Now to show we observe the following equivalence

$$\begin{aligned} f \equiv g_n h_n \pmod{\pi^n} &\Leftrightarrow f \equiv g_{n-1} h_{n-1} + \pi^{n-1}(g_{n-1}v + h_{n-1}u) + \pi^{2n-2}uv \pmod{\pi^n} \\ &\Leftrightarrow f \equiv g_{n-1} h_{n-1} + \pi^{n-1}(g_{n-1}v + h_{n-1}u) \pmod{\pi^n} \\ &\Leftrightarrow f - g_{n-1} h_{n-1} \equiv \pi^{n-1}(g_{n-1}v + h_{n-1}u) \pmod{\pi^n} \\ &\Leftrightarrow w := \frac{f - g_{n-1} h_{n-1}}{\pi^{n-1}} \equiv g_{n-1}v + h_{n-1}u \pmod{\pi} \end{aligned}$$

for the last equality comes from the observation that

$$x \equiv \pi^{n-1}y \pmod{\pi^n} \Leftrightarrow x = \pi^{n-1}y + \pi^n z \Leftrightarrow x/\pi^{n-1} = y + \pi z \Leftrightarrow x/\pi^{n-1} \equiv y \pmod{\pi}$$

We now start to actually find $u, v \in \mathcal{O}[t]$. Because g_1 is monic, by Euclidean algorithm for polynomials, we have that $w\beta = g_1 q + u$ in $\mathcal{O}[t]$ with $d_u < d_{g_1}$.

$$\alpha g_1 + \beta h_1 \equiv 1 \Leftrightarrow w\alpha g_1 + w\beta h_1 \equiv w \pmod{\pi}$$

Plugging in $w\alpha g_1 + (g_1 q + u)h_1 \equiv w \Rightarrow (w\alpha + qh_1)g_1 + uh_1 \equiv w \pmod{\pi}$. Denote v to be the polynomial obtained by replacing all coefficient of $w\alpha + qh_1$ that is divisible by π into 0. We still get the modulo equivalence $\alpha v + \beta u = w$, and gives us i).

We are left to prove iv).

$$d_u < d_{g_1} \Rightarrow d_{g_n} = \deg(g_{n-1} + \pi^{n-1}u) = d_{g_{n-1}} = d_G$$

Suppose for contradiction that $d_{h_n} > d_f - d_G$,

$$h_n = h_{n-1} + \pi^{n-1}v \text{ and } d_{h_{n-1}} \leq d_f - d_G \Rightarrow d_v > d_f - d_G$$

$$d_{g_{n-1}} = d_G \text{ and } d_{h_{n-1}} \leq d_f - d_G \Rightarrow \deg(f - g_{n-1}h_{n-1}) \leq d_f \Rightarrow w \leq d_f$$

Now we come back to the equality $vg_1 + uh_1 \equiv w \pmod{\pi}$. Because $\deg(vg_1) \geq \deg(uh_1)$, we have that the leading coefficient of $vg_1 + uh_1$ is not divisible by π . However, because $d_w < d_{vg_1}$ we have that

$$vg_1 + uh_1 = w + \pi\gamma$$

for some γ with $d_\gamma > w$. The right hand side has leading coefficient divisible by π leading into contradiction.

For all i , we have $g_i(x) = a_0^{(i)} + \cdots + a_{r-1}^{(i)}t^{r-1} + t^r$ with $r = d_G$. First let $m \geq n \geq N$, then we claim that

$$a_j^{(n)} \equiv a_j^{(m)} \pmod{\pi^N}$$

which can be easily established by induction from $a_j^{(n)} \equiv a_j^{(n-1)} \pmod{\pi^{n-1}}$. Furthermore, we define $\varphi(x) = e^{-v(x)}$. Let $q = e^{-\varepsilon}$, then

$$\pi^N |x \Leftrightarrow v(x) \geq v(\pi)^N = N\varepsilon \Leftrightarrow e^{-v(x)} \leq e^{-N\varepsilon} \Leftrightarrow \varphi(x) \leq q^N$$

Thus we have that $\{a_j^{(i)}\}$ is a Cauchy sequence for fixed j , hence converges to $a_j \in \mathcal{O}$ as F is \mathfrak{p} -complete. For $n \geq i$,

$$\varphi(a_j^{(i)} - a_j^{(n)}) \leq q^i \Rightarrow \varphi(a_j^{(i)} - a_j) \leq q^i \Rightarrow a_j - a_j^{(i)} \equiv 0 \pmod{\pi^i}$$

Clearly, if $a \equiv 0 \pmod{\pi^i} \Rightarrow \varphi(a) < q^i$ for all i , thus $\varphi(a) = 0 \Rightarrow a = 0$. We can finally conclude that

$$f \equiv g_i h_i \equiv gh \pmod{\pi^i} \text{ for all } i \Rightarrow f = gh$$

$d_g = d_{g_i} = d_G$ with $\bar{g} = \bar{g}_i = G$ and $\bar{h} = \bar{h}_i = H$ complete our proof. \square

Corollary 7.2. *If $f = a_0 + \cdots + a_n t^n \in F[t]$ is irreducible, then $\bar{v}(f) = \min(v(a_0), \dots, v(a_n)) = \min(v(a_0), v(a_n))$. In particular, if f is monic and irreducible, i.e. $a_n = 1$, then*

$$f \in \mathcal{O}[t] \Leftrightarrow a_0 \in \mathcal{O}$$

Proof. First f primitive has the following equivalences

$$f \text{ primitive} \Leftrightarrow a_j \notin \mathfrak{p} \Leftrightarrow v(a_j) = 0 \Leftrightarrow \bar{v}(f) = 0$$

where a_j is some coefficient in f . If $\bar{v}(g) = \alpha \neq 0$, then $\bar{v}(g/\alpha) = 0$, hence all polynomial has the form $g = \alpha f$ where f is primitive. If we have proved the result for primitive polynomials, then

$$\bar{v}(g) = \bar{v}(\alpha f) = \bar{v}(\alpha) + \bar{f} = \bar{v}(\alpha) + \min(v(a_0), v(a_n)) = \min(v(\alpha a_0), v(\alpha a_n))$$

So we may assume f to be primitive. Now suppose $\min(v(a_0), v(a_n)) > 0$, then there exists r such that $v(a_r) = 0$, $v(a_i) > 0$ for $i \geq r$ and $0 < r < n$. The existence follows from $\bar{v}(f) = 0$. $\bar{f} = \bar{f} \cdot 1 = GH$ modulo \mathfrak{p} . But $d_G = r < n$ gives contradiction.

Now further suppose that f is monic, then $\bar{v}(f) = \min(v(1), v(a_0)) = v(a_0)$, so if $v(a_0) \geq 0 \Rightarrow v(a_i) \geq 0$ for all i . $\bar{v}(f) \geq 0 \Leftrightarrow f \in \mathcal{O}[t]$ completes the proof. \square

8. PRODUCT FORMULA

If k is a number field, \mathcal{O}_k is the algebraic integer of k with $\mathfrak{p} \subset \mathcal{O}_k$ a prime ideal. Let $\mathfrak{p} | p$, then we say that \mathfrak{p} **lies over** $p \in \mathbb{Z}$. If the prime number is indexed with i , i.e. \mathfrak{p}_i , then we denote its corresponding exponential valuation v_i . Also, we note its corresponding valuation by φ_i .

Recall that we may define the absolute norm of $N : J_k \rightarrow \mathbb{Q}$ where J_k is the group of all fractional ideals of k by $\mathfrak{A} \mapsto |\mathcal{O}/\mathfrak{A}|$. Many classical textbooks show that N is indeed extended from the norm from k to \mathbb{Q} in that if $x \in k$, and (x) is the principal ideal generated by x , then

$$N((x)) = |N_{\mathbb{Q}}^k(x)|$$

Proposition 8.1. *Let $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ be lying over p , and let φ_i and φ be the corresponding valuations respectively, then we have*

$$\varphi(N(x)) = \prod_{i=1}^m \varphi_i(x)$$

Proof. By the unique factorization,

$$(x) = \prod_{i=1}^m \mathfrak{p}_i^{n_i} \times \mathfrak{A}$$

where \mathfrak{A} is relatively prime to \mathfrak{p}_i for all i . By definition $v_i(x) = n_i$ where v_i is the corresponding exponential valuation of \mathfrak{p}_i , hence with $f_i = [\mathcal{O}_k/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}]$, we have that $\varphi_i(x) = p^{-f_i n_i}$. Then we have that

$$\prod_{i=1}^m \varphi_i(x) = p^{-\sum f_i n_i}$$

On the other hand, we have that

$$N(x) = \prod_{i=1}^m N(\mathfrak{p}_i)^{n_i} \times N(\mathfrak{A}) = p^{\sum f_i n_i} \times N(\mathfrak{A})$$

because \mathfrak{A} is the product of power of primes other than p , we have that

$$\varphi(N(x)) = p^{-\sum f_i n_i}$$

hence we may conclude the proof. □

Theorem 8.2. *Let $x \in k^*$, then we have*

$$\prod_{v \in M_k} \varphi_v(x)^{n_v} = 1$$

where $n_v = 1$ when v is nonarchimedean or real archimedean, and $n_v = 2$ when v is complex archimedean.

Proof. We first let $k = \mathbb{Q}$, then by multiplicity we prove for $x = p$, a prime number. Let φ_q be the valuation for prime q , then

$$\varphi_q(p) = \begin{cases} 1/p & \text{if } q = p \\ 1 & \text{if } q \neq p \end{cases}$$

Then clearly,

$$\prod_{v \in M_{\mathbb{Q}}} \varphi_v(p)^{n_v} = |p| \varphi_p(p) = |p|/p = 1$$

Now for general number field k , we have that

$$\begin{aligned}
\prod_{v \in M_k} \varphi_v(x)^{n_v} &= \prod_{v \in M_k \setminus S_\infty} \varphi_v(x) \prod_{v \in S_\infty} \varphi_v(x)^{n_v} \\
&= \prod_{v \in M_k \setminus S_\infty} \varphi_v(x) |N(x)| \\
&= \prod_{\mathfrak{p}} \varphi_{\mathfrak{p}}(x) |N(x)| \\
&= \prod_p \prod_{\mathfrak{p} | p} \varphi_{\mathfrak{p}}(x) |N(x)| \\
&= \prod_p \varphi_p(N(x)) |N(x)| \\
&= \prod_{v \in M_{\mathbb{Q}}} \varphi_v(N(x)) = 1
\end{aligned}$$

□

Lemma 8.3. *Let $v_1, v_2 \in M_k$ with k a number field be two distinct valuation in M_k , then there exists $x \in k$ such that $\varphi_1(x) > 1$ and $\varphi_2(x) < 1$.*

Proof. Let $v_1 = v_{\mathfrak{p}}$ and $v_2 = v_{\mathfrak{q}}$ where $\mathfrak{p}, \mathfrak{q}$ are two distinct prime ideals of \mathcal{O}_k . Consider an element $x \in \mathfrak{q} \setminus \mathfrak{p}$ and $y \in \mathfrak{p} \setminus \mathfrak{q}$. Then we have $\varphi_{\mathfrak{p}}(x) > 1$ and $\varphi_{\mathfrak{q}}(x) \leq 1$. If $\varphi_{\mathfrak{q}}(x) \neq 1$, then x works. If $\varphi_{\mathfrak{p}}(y) \neq 1$, then we have that y^{-1} works. If both $\varphi_{\mathfrak{p}}(x) = \varphi_{\mathfrak{q}}(y) = 1$, then xy^{-1} works.

Let $v_1 = \sigma$ for some $\sigma \in \text{Hom}(k, \mathbb{C})$, and $v_2 = v_{\mathfrak{p}}$ then we consider $x \in \mathfrak{p} \cap \mathbb{Z}$. $\varphi_1(x) > 1$ and $\varphi_2(x) < 1$ as inverse of a rational integer is never integral. If v_1 is nonarchimedean and v_2 is archimedean, then x^{-1} will for $x \in \mathfrak{p} \cap \mathbb{Z}$.

Now for v_1, v_2 both archimedean, we know that it arises from different complex embeddings of k , we see that there exists $x \in k$ such that $\varphi_1(x) \neq \varphi_2(x)$. Without loss of generality, suppose that there exists r such that $\varphi_1(x) < r < \varphi_2(x)$, then we see that

$$\varphi_1(r/x) > 1 \quad \text{and} \quad \varphi_2(r/x) > 1$$

□

We have seen the equivalence

$$\varphi(x) < 1 \Leftrightarrow x \in B_{\varphi}(0, 1)$$

so we have that for two distinct v_1 and v_2 , the open ball centered at 0 of radius 1 is different for all v , i.e. v_1 and v_2 are inequivalent.

Lemma 8.4. *Suppose v_1 and v_2 are two distinct elements in M_k . Suppose $x \in k$ satisfies $\varphi_1(x) > 1$ and $\varphi_2(x) < 1$, then the sequence*

$$z_m = \frac{x^m}{1 + x^m}$$

converges to 1 with respect to v_1 and converges to 0 with respect to v_2 .

Proof. By performing the same procedure, we get the *usual* theorems of limit, i.e., given x_n, y_n sequences in k , and a valuation φ of k , suppose $x_n \rightarrow x$ and $y_n \rightarrow y$, then

- i) $\varphi(x_n + y_n) \rightarrow x + y$,
- ii) $\varphi(x_n y_n) \rightarrow xy$,

iii) $\varphi(x_n/y_n) \rightarrow x/y$ for $y_n \neq 0$ for all n and $y \neq 0$.

In particular, $\varphi_2(x^m/(1+x^m)) = \varphi_2(x^m)/\varphi_2(1+x^m) \rightarrow 0/1 = 0$. Also, we get $\varphi_1(x) > 1 \Rightarrow \varphi_1(1/x) < 1 \Rightarrow$

$$\varphi_1\left(\frac{x^m}{1+x^m}\right) = \varphi_1\left(\frac{1}{\frac{1}{x^m}+1}\right) = 1/\varphi_1\left(\frac{1}{x^m}+1\right) \rightarrow 1/1 = 1$$

□

Theorem 8.5 (Approximation theorem). *For distinct $v_1, \dots, v_s \in M_k$, $x_1, \dots, x_s \in k$, not necessarily distinct, and $\varepsilon > 0$, there exists $x \in k$ such that*

$$\varphi_i(x - x_i) < \varepsilon$$

for all $i = 1, \dots, s$.

Proof. We first show that there exists y_i such that $\varphi_i(y_i) > 1$ and $\varphi_j(y_i) < 1$ for all $j \neq i$. We have proved the case when $i = 2$, so we may proceed by induction. Also, without loss of generality, we may assume that $i = 1$. So suppose by inductive hypothesis we have y such that

$$\varphi_1(y) > 1 \text{ and } \varphi_i(y) < 1$$

for $i = 1, \dots, s-1$. If $\varphi_s(y) < 1$, then we are done, so first we assume that $\varphi_s(y) = 1$. Let $z \in k$ be such that $\varphi_1(z) > 1$ and $\varphi_s(z) < 1$. Then we can let m large enough so that $y^m z$ works, so we are left with the case where $\varphi_s(y) > 1$. We then let

$$z_m = \frac{y^m}{1+y^m}$$

which converges to 1 with respect to both v_1 and v_2 , and z_m will converge to 0 with respect to v_2, \dots, v_{s-1} . Pick z such that $\varphi_1(z) > 1$ and $\varphi_s(z) < 1$, then for sufficiently large m , we see that $z_m z$ works.

Now we are given y_i such that

$$\varphi_i(y_i) > 1 \quad \text{and} \quad \varphi_j(y_i) < 1 \text{ for } j \neq i$$

Then letting $z_i = y_i/(1+y_i)$ for some appropriate l , we see that z_i is arbitrary closed 1 with respect with v_i and arbitrary close to 0 with respect with v_j with $j \neq i$. By letting $x = z_1 x_1 + \dots + z_s x_s$ with the inequality

$$\varphi_i(x - x_i) \leq \varphi_i(z_1)\varphi_i(x_1) + \dots + \varphi_i(z_i - 1)\varphi_i(x_i) + \dots + \varphi_i(z_s)\varphi_i(x_s)$$

can be arbitrary small. □

Part 3. Adeles and Ideles

9. RESTRICTED PRODUCT

Let G be a topological group, with $*$: $G \times G \rightarrow G$ denote its continuous multiplication. For any $g \in G$, we define

$$i_g : G \rightarrow G \times G \text{ defined by } h \mapsto (g^{-1}, h)$$

For any open set $U \times V \subset G \times G$, with U, V open in G , we have $i_g^{-1}(U \times V) = V$ if $g^{-1} \in U$ and \emptyset otherwise. This shows that i_g is continuous. The composition

$$G \xrightarrow{i_g} G \times G \xrightarrow{*} G$$

which sends $h \in G$ to $g^{-1}h$, we see that the preimage of a subset H of G is simply gH . Hence for any open set $H \subset G$, we get gH is also open by continuity.

Let G_v be a locally compact topological groups with $K_v \subset G_v$ be compact subsets which is defined for almost all v . We use M_G be the set of indices, and $S_\infty \subset M_G$ be the subset which consists of all indices where K_v is not defined. A **restricted product** \mathbb{I}_G of G_v with respect to K_v is a subset of the direct product

$$\prod G_v$$

consisting of $(x_v) \in \prod G_v$ where $x_v \in K_v$ for almost all v , i.e. for all but finitely many v . We do not give \mathbb{I}_G the subspace topology, but we consider the subset

$$\prod_{v \in S} U_v \times \prod_{v \notin S} K_v$$

where $U_v \subset G_v$ open sets and $S \subset M_G$ be a finite subset containing S_∞ to be the basis of the topology for J . The simplest set of this form is

$$\mathbb{I}_S = \underbrace{\prod_{v \in S} G_v}_{(1)} \times \underbrace{\prod_{v \notin S} K_v}_{(2)}$$

(1) is locally compact as S is finite and (2) is compact by Tychonoff, so the total product is locally compact. (The space itself is the compact neighborhood of every point in the space.) We easily see that

$$\mathbb{I}_G = \bigcup_{\substack{S_\infty \subset S \\ S \text{ finite}}} \mathbb{I}_S$$

hence for all $x \in \mathbb{I}_G$, there exists a compact neighborhood $K_i \subset \mathbb{I}_S$ of x for some \mathbb{I}_S containing x , as \mathbb{I}_S is locally compact. \mathbb{I}_G is itself locally compact. Because we haven't used any properties of G_v being topological groups, we may generalize the construction to simply collection of X_v locally compact topological spaces with K_v compact subsets with a locally compact restricted product \mathbb{I}_X .

Proposition 9.1. *Let G_v be a locally compact set with K_v be a compact subset of G_v defined for almost of $v \in M_G$ with M_G for some indexing set, then the restricted product of G_v with respect to K_v is a topological group. Furthermore, if G_v are topological rings (resp. topological fields), then the restricted product is also a topological ring.*

Proof. Let f be an operation whether it be $+$ or $*$, then consider an open set

$$\left(\prod U_v \times \prod \mathcal{O}_v \right) \times \left(\prod U'_v \times \prod \mathcal{O}_v \right) = \prod (U_v \times U'_v) \times \prod (\mathcal{O}_v \times \mathcal{O}_v)$$

then its preimage will have the form

$$\prod f_v^{-1}(U_v \times U'_v) \times \prod f_v^{-1}(\mathcal{O}_v \times \mathcal{O}_v)$$

where $f = \prod f_v$ with $f_v : G_v \rightarrow G_v \times G_v$, the operation function for each component. We know that the preimages are open as k_v are all topological rings. The same reasoning works for negation. \square

We have shown that for all $v \in M_k$ where k is a number field, k_v is locally compact. For all nonarchimedean prime divisors v , we have a compact subset \mathcal{O}_v of k_v . The restricted product of k_v with respect to \mathcal{O}_v will be called the **adeles** of k , denoted \mathbb{A}_k . If we have compact subsets \mathcal{O}_v^* with k_v^* , then the restricted product will be called the **ideles** of k and will be denoted \mathbb{I}_k .

10. FINITENESS AND UNIT THEOREM

Let $\varphi : \mathbb{I}_k \rightarrow \mathbb{R}^{>0}$ be a map defined by

$$x \mapsto \prod_v \varphi_v(x_v)$$

then the map is clearly an epimorphism. Because for any element, we can adjust one of the archimedean valuations. The next step is to show that the map is continuous. We first prove a lemma that the product of positive reals slightly changes if each term changes slightly. Let (b_1, b_2) be an interval in \mathbb{R} . For any $x \in \mathbb{I}_k$ such that $\varphi(x) \in (a, b)$ and let S be the finite subset of M_k containing all valuations such that $\varphi_v(x_v) \neq 1$ then we have

$$\prod_{v \in M_k} \varphi_v(x_v) = \prod_{v \in S} \varphi_v(x_v)$$

then by A.2, there exists $\varepsilon \in \mathbb{R}$ such that

$$b_1 < \prod_{v \in S} \varphi_v(x_v) - \varepsilon \text{ and } \prod_{v \in S} \varphi_v(x_v) + \varepsilon < b_2$$

Now consider the open set

$$U = \prod_{v \in S} B(x_v, \varepsilon) \times \prod_{v \notin S} \mathcal{O}_k^*$$

Clearly $x \in U$, and for any $y \in U$,

$$\varphi(y) = \prod_{v \in S} \varphi_v(y_v) = \prod_{v \in S} \varphi_v(y_v - x_v + x_v) \leq \prod_{v \in S} \varphi_v(x_v) + \varphi_v(x_v - y_v) \leq \prod_{v \in S} \varphi_v(x_v) + \varepsilon < b_2$$

The reverse triangle inequality implies that

$$\begin{aligned} |\varphi_v(x_v) - \varphi_v(y_v)| &\leq \varphi_v(x_v - y_v) \Rightarrow \varphi_v(x_v) - \varphi_v(y_v) \leq \varphi_v(x_v - y_v) \\ &\Rightarrow \varphi_v(x_v) \leq \varphi_v(x_v - y_v) + \varphi_v(y_v) \Rightarrow \varphi_v(x_v) - \varphi_v(x_v - y_v) \leq \varphi_v(y_v) \end{aligned}$$

$$\varphi(y) = \prod_{v \in S} \varphi_v(y_v) \geq \prod_{v \in S} \varphi_v(x_v) - \varphi_v(x_v - y_v) \geq \prod_{v \in S} \varphi_v(x_v) - \varepsilon > b_1$$

which shows that U is a subset of the preimage of (a, b) . We, thus, have shown that the preimage is open and that the map is continuous. Clearly, $\{1\} \subset \mathbb{R}^{>0}$ is closed, the $\ker(\varphi)$ is closed and will be denoted \mathbb{I}_k^0 .

The second map to consider is a map from the ideles to the fractional ideals of k^* denoted, J_k ,

$$\psi : \mathbb{I}_k \rightarrow J_k$$

then the map is defined by

$$x \mapsto \prod_{v_p \in M_k \setminus S_\infty} \mathfrak{p}^{v_p(x_{v_p})}$$

For any fractional ideal

$$\prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$$

we have an element $x = (x_v)$ in the preimage by setting $x_v = e_{\mathfrak{p}}$ if $v = v_{\mathfrak{p}}$ and $x_v = 1$ otherwise. This shows that the map is surjective. The kernel of this map consists of elements such that $\varphi_v(x_v) = 1$ for all $v \in S_{\infty}$. For $x \in k^*$, we have that $\psi(x) = (x)$ where the latter is the principal ideal generated by x . If we denote P_k to be the principal ideals of k^* , then we get an induced surjective map

$$\mathbb{I}_k/k^* \rightarrow J_k/P_k$$

with $\mathbb{I} \rightarrow J_k/P_k$. The kernel of the ψ is clearly $\mathbb{I}_{S_{\infty}}$.

Claim 10.1. *We get an isomorphism*

$$\mathbb{I}_k/k^*\mathbb{I}_{S_{\infty}} \cong J_k/P_k = Cl_k$$

where Cl_k is the ideal class group.

Proof. Let αx be such that $\alpha \in k^*$ and $x \in \mathbb{I}_{S_{\infty}}$, then consider the ideal (αx) . Because $(\alpha x) = (\alpha)(x)$, in the image, it is equivalent to (x) . $x \in \mathbb{I}_{S_{\infty}}$ implies that (x) is, in fact, \mathcal{O}_k . Now conversely, suppose $x \in \mathbb{I}_k$ be such that $(x) \in P_k$, then there exists $\alpha \in k^*$ such that $(x) = (\alpha)$. We have that $(x\alpha^{-1}) = \mathcal{O}_k$. We know that $x\alpha^{-1} \in \mathbb{I}_{S_{\infty}}$, hence $x\alpha^{-1} = y$ for some $y \in \mathbb{I}_{S_{\infty}}$. We conclude that $x = \alpha y$, hence the kernel is $k^*\mathbb{I}_{S_{\infty}}$. \square

Similar to the ideal class group, we have $C_k = \mathbb{I}_k/k^*$ and call it the **idele class group**. The relationship between the two class groups can be drawn from the epimorphism

$$C_k \rightarrow Cl_k$$

For any finite set S containing S_{∞} , we denote $k_S = \mathbb{I}_S \cap k^*$ called the **S -units** of k . C_k is generalized to

$$C_S = \mathbb{I}_S/k_S$$

We will call C_S the **S -idele class group**.

Claim 10.2. *The kernel of $C_k \rightarrow Cl_k$ is $C_{S_{\infty}}$.*

Proof. The kernel is the image of $k^*\mathbb{I}_{S_{\infty}}$ under \mathbb{I}_k/k^* , then k^* cancels, and we are left with $\mathbb{I}_{S_{\infty}}$. This shows that the kernel is $\mathbb{I}_{S_{\infty}}/k_{S_{\infty}}$ which is $C_{S_{\infty}}$. \square

We restrict the domain of the function by considering \mathbb{I}_k^0 . We denote

$$\mathbb{I}_S^0 = \mathbb{I}_S \cap \mathbb{I}_K^0$$

$$C_S^0 = \mathbb{I}_S^0/k_S$$

Claim 10.3. *The map is still surjective when we shrink the domain from C_k to C_k^0 with its kernel $C_{S_{\infty}}^0$*

Proof. The first goal is to prove that $C_k^0 \rightarrow Cl_k$ is surjective. Let \mathfrak{A} be a fractional ideal of k , then by the surjectivity of the original map, there exists $x \in \mathbb{I}_k$ such that $(x) = \mathfrak{A}$. Consider $\phi(x)$, then we can change x by one of its archimedean properties and get x' so that $\phi(x') = 1$. $C_k = \mathbb{I}_k/k^*$ implies that $x' \in C_k^0$.

As we can view $C_k^0 \subset C_k$, the kernel is clearly $\mathbb{I}_{S_{\infty}}^0/k_{S_{\infty}}$ which is $C_{S_{\infty}}^0$. \square

The claims above combine to establish the isomorphism

$$C_k^0/C_{S_\infty}^0 \cong C_k$$

Before we prove the topological property of C_k^0 , consider the following notation, for any $x \in \mathbb{I}_k$,

$$L(x) := \{\alpha \in k^* \mid |\alpha|_v \leq |x_v|_v \text{ for all } v \in M_k\}$$

Let $\lambda(x) = |L(x)|$, the order, then what we want to show is that if $|x|$ is sufficiently large, then $\lambda(x) > 0$. Observe that $L(x)$ has a canonical bijection with $L(\alpha x)$ for any $\alpha \in k^*$ by

$$y \mapsto \alpha y$$

Proposition 10.4 (Stronger Approximation Theorem). *Let k be a number field, then there exists c_k which is depended only on k such that for all $x \in \mathbb{I}_k$,*

$$\lambda(x) \geq c_k \varphi(x)$$

Proof. Let $n = [k : \mathbb{Q}]$ and w_1, \dots, w_n be the integral basis of \mathcal{O}_k , then define

$$c := \sup_{v \in S_\infty, i} (\varphi_v(w_i))$$

Then the above immediately implies that

$$\varphi_v(w_1) + \dots + \varphi_v(w_n) \leq c$$

Let $a_v = c/\varphi_v(x_v)$, then $a_v < 2a_v$, so there exists $r_v \in \mathbb{Q}$ and $\varepsilon \in \mathbb{R}^{>0}$ such that $(r - \varepsilon, r + \varepsilon) \subset (a_v, 2a_v)$, then by the approximation theorem, there exists $\alpha \in k^*$ such that

$$\varphi_v(\alpha - r_v) < \varepsilon$$

for all $v \in S_\infty$, then

$$|\varphi_v(\alpha) - \varphi_v(r_v)| \leq \varphi_v(\alpha - r_v) < \varepsilon$$

we get

$$\varphi_v(r_v) - \varepsilon < \varphi_v(\alpha) < \varphi_v(r_v) + \varepsilon$$

which implies

$$\frac{c}{\varphi_v(x_v)} < \varphi_v(\alpha) < \frac{2c}{\varphi_v(x_v)}$$

Now for αx , consider all finite v such that $\varphi_v(\alpha x_v) > 1$. By letting m be divisible *highly* by all v , we see that $\varphi_v(m\alpha x) \leq 1$ for all nonarchimedean v , i.e. for all $v \in M_k \setminus S_\infty$. Let $z = m\alpha x$, then we have

$$mc < \varphi_v(z_v) < 2mc \text{ for } v \in S_\infty \text{ and for some } m \in \mathbb{Z},$$

$$\varphi_v(z_v) \leq 1 \text{ for } v \in M_k \setminus S_\infty$$

By the second inequality, we have that (z) , the fractional ideal corresponding to z is an integral ideal of k . Hence we have that $N(z) = |\mathcal{O}_k/(z)|$. Let $\Gamma := \{y \in \mathcal{O}_k \mid y = a_1 w_1 + \dots + a_n w_n, 0 \leq a_i \leq m\}$. Then Γ has $(m+1)^n$ elements. By the pigeonhole principal, we see that there exists an equivalence class in $\mathcal{O}_k/(z)$ with more than $m^n/N(z)$ elements. In fact, if all equivalence classes have less than $m^n/N(z)$, we have $|\Gamma| \leq m^n/N(z) \cdot N(z) = m^n < (m+1)^n = |\Gamma|$. We thus have a $\Gamma' \subset \Gamma$ with more than $m^n/N(z)$ elements which fall into the same equivalence

class. Let $y_1 \in \Gamma'$ be fixed, and we vary $y_2 \in \Gamma'$.

If $y_1 = \sum a_i w_i$ and $y_2 = \sum b_i w_i$,

$$\begin{aligned} \varphi_v(y_1 - y_2) &= \varphi_v \left(\sum a_i w_i - \sum b_i w_i \right) \\ &= \varphi_v \left(\sum (a_i - b_i) w_i \right) \\ &\leq \sum \varphi_v(a_i - b_i) \varphi_v(w_i) \\ &\leq m \sum \varphi_v(w_i) \leq mc \leq \varphi_v(z_v) \end{aligned}$$

for all v archimedean. We had that $-m \leq a_i - b_i \leq m$. Because $y_1 - y_2, z_v \in \mathcal{O}_k$, we see that $y_1 - y_2 \in (z) \Rightarrow \varphi_v(y_1 - y_2) \leq \varphi_v(z_v)$ for nonarchimedean v . This is because $y_1 - y_2$ is more divisible by \mathfrak{p} than z_v . $y_1 - y_2 \in L(z)$, so

$$m^n / N(z) \leq |\Gamma'| \leq \lambda(z) \Rightarrow 1/N(z) \leq \lambda(z) m^{-n}$$

For any $z \in \mathbb{I}_k$, we have that

$$\prod_{v \in M_k \setminus S_\infty} \varphi_v(z_v) = \prod_{i=1}^n \prod_{\mathfrak{p} | p_i} \varphi_{\mathfrak{p}}(z_{\mathfrak{p}}) = \prod_{i=1}^n p_i^{-\sum f_{\mathfrak{p}} n_{\mathfrak{p}}} = 1/N(z)$$

Hence

$$\varphi(z) = \prod_{v \in M_k \setminus S_\infty} \varphi_v(z_v) \prod_{v \in S_\infty} \varphi_v(z_v) = 1/N(z) \prod_{v \in S_\infty} \varphi_v(z_v) \leq \lambda(z) m^{-n} (2mc)^n = \lambda(z) 2^n c^n$$

We conclude that

$$\lambda = (2^n c^n)^{-1} \varphi(z)$$

Because $m\alpha \in k^*$, we see that $\varphi(z) = \varphi(x)$ by the product formula and $\lambda(x) = \lambda(z)$, hence letting $c_k = (2^n c^n)^{-1}$ \square

Lemma 10.5. *Let $x \in \mathbb{I}_k$ with $\varphi(x) \geq 2/c_k$, then there exists $\alpha \in k^*$ such that*

$$1 \leq \varphi_v(\alpha x_v) \leq \varphi(x)$$

for all $v \in M_k$.

Proof. We have $2 \leq c_k \varphi(x) \leq \lambda(x)$, then there exists $\beta \in \lambda(x)$ nonzero such that $\varphi_v(\beta) \leq \varphi_v(x_v)$ for all $v \in M_k$. Consider $\alpha = \beta^{-1}$, then

$$1 \leq \varphi_v(\alpha x_v)$$

and

$$\varphi_v(\alpha x_v) = \frac{\prod_w \varphi_w(\alpha x_w)}{\prod_{w \neq v} \varphi_w(\alpha x_w)} \leq \frac{\varphi(\alpha x)}{1} = \varphi(\alpha x) = \varphi(x)$$

In fact,

$$1 \leq \varphi_w(\alpha x_w) \Rightarrow 1 \leq \prod_{w \neq v} \varphi_w(\alpha x_w)$$

\square

Proposition 10.6. \mathcal{C}_k^0 is compact

Proof. By the product formula, $\varphi(x) = 1$, so we get a well-defined map

$$\varphi : C_k \rightarrow \mathbb{R}^{\geq 0}$$

with the kernel C_k^0 , because it is the image of \mathbb{I}_k^0 under \mathbb{I}_k/k^* . First we show that for any $\rho \in \mathbb{R}^{\geq 0}$, $\varphi^{-1}(\rho)$ is homeomorphic to C^0 . Let $x_\rho \in \mathbb{I}_k$ be such that $\varphi(x_\rho) = \rho$. We can find such by modifying it by one of its archimedean components. Then we see that $\varphi^{-1}(\rho) = x_\rho C_k^0$. In fact,

$$\varphi(x_1) = \varphi(x_2) \Rightarrow x_1 x_2^{-1} \in \ker(\varphi) = C_k^0 \Rightarrow x_1 \in x_2 C_k^0$$

thus homeomorphic as \mathbb{I}_k is a topological group.

Choose $\rho > 2/c_k$ and pick $x \in \varphi^{-1}(\rho)$, then by the stronger approximation theorem, we get $\alpha_x \in k^*$ such that

$$1 \leq \varphi_v(\alpha_x x_v) \leq \rho$$

for all $v \in M_k$. We have that v_p takes no values between 1 and p^f where $(p) = \mathfrak{p} \cap \mathbb{Z}$ and $f = [\mathcal{O}_k/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$, and there are only finitely many primes \mathfrak{p} such that $p^f \leq \rho$, hence we have that

$$\begin{aligned} 1 &\leq |\alpha_x x_v|_v \leq \rho \text{ for } v \in S \\ |\alpha_x x_v|_v &= 1 \text{ for } v \notin S \end{aligned}$$

for some $S_\infty \subset S \subset M_k$ finite subset. We define

$$T = \prod_{v \in S} \left(\overline{B(0, \rho)} - B(0, 1) \right) \times \prod_{v \notin S} \mathcal{O}_v^*$$

then as each term is compact, we have T compact by Tychonoff. $\varphi^{-1}(\rho)$ is contained inside the image of T as we can change the elements in $\varphi^{-1}(\rho)$ by elements in k^* . The image of T is compact and $\varphi^{-1}(\rho)$ is a closed subset of compact space T . $\varphi^{-1}(\rho)$ is compact. \square

Theorem 10.7. *The class group Cl_k for a number field k is finite.*

Proof. $C_{S_\infty}^0$ is an open subset of C_k^0 , hence $C_k^0/C_{S_\infty}^0$ is discrete, and compact as C_k^0 is compact. $\{\{x\}\}_{x \in X}$ is an open covering where $X = C_k^0/C_{S_\infty}^0$. By compactness, there exists a finite subcover, i.e. $C_k^0/C_{S_\infty}^0$ is finite. The isomorphism

$$C_k^0/C_{S_\infty}^0 \cong Cl_k$$

implies that Cl_k is finite. \square

Theorem 10.8 (Dirichlet S -Unit Theorem). *For any finite set $S \subset M_k$, k_S has rank $s - 1$ where $s = |S|$.*

Proof. Consider the log map on ideles

$$\log : \mathbb{I}_S \rightarrow \mathbb{R}^s$$

defined by

$$\log(x) = (\log \varphi_1(x_1)^{n_1}, \dots, \log \varphi_s(x_s)^{n_s})$$

where φ_i corresponds to $v_i \in S$, and x_i is the v_i -component of $x \in \mathbb{I}_S$. Also, n_i is 1 or 2 depending whether φ_i is real or complex embedding, respectively. As each component is a composition of continuous maps, they are continuous. Consequently, \log is continuous.

By definition $x \in \mathbb{I}_S^0$ implies that $\varphi(x) = 1$ and $\varphi_v(x_v) = 1$ for $v \notin S$. It

follows that $\log(\mathbb{I}_S^0)$ lies inside the hyperplane H which is composed of elements $(y_1, \dots, y_s) \in \mathbb{R}^s$ such that

$$y_1 + \dots + y_s = 0$$

We may, without loss of generosity, assume that v_s is archimedean. The following $n - 1$ vectors

$$\begin{pmatrix} a_1, 0, \dots, 0, -a_1 \\ 0, a_2, \dots, 0, -a_2 \\ \vdots \\ 0, 0, \dots, a_{s-1}, -a_{s-1} \end{pmatrix}$$

are linearly independent for a_i nonzero. We conclude that $\dim_{\mathbb{R}}(H) = s - 1$. Because all vectors lies inside $\log(\mathbb{I}_S^0)$, we have just proved that it generates H .

Claim 10.9. $\log(k_S)$ is discrete in \mathbb{R}^s .

Proof. Let T be a bounded subset of \mathbb{R}^n , then the value of archimedean valuation on $\log(k_S) \cap T$ is bounded. If the coefficient of polynomials over \mathbb{Z} that satisfies an element in k^* is not bounded, then we need a $x \in k$ with a bigger valuation to make $f(x) = 0$. The coefficients of f is thus bounded. Because the coefficients are in \mathbb{Z} and the degree is bounded by $[k : \mathbb{Q}]$, we have only finitely many such polynomials. Note that we don't have to assume that the polynomial is monic, hence all elements in k satisfies some polynomial with coefficient in \mathbb{Z} . $T \cap \log(k_S)$ is, thus, finite. \square

Claim 10.10. Let X be a discrete subset of \mathbb{R}^s , then it is free abelian of rank $\dim(\mathbb{R}X)$ where $\mathbb{R}X$ is the \mathbb{R} -span of X .

Proof. We use induction on the dimension of $\mathbb{R}X$. If $\dim(\mathbb{R}X) = 1$, then X discrete implies that there exists nonzero $x \in X$ such that x is closest to 0. Now suppose X is generated by y which exists as $\dim(\mathbb{R}X) = 1$. $y = kx$ for some $k \in \mathbb{R}$. There exists $t \in \mathbb{Z}$ such that $|k - t| < 1$. Then $ty - x$ is closer to 0 than x which contradicts the minimality of x .

We now assume that $\dim(\mathbb{R}X) = m > 1$ with basis x_1, \dots, x_m of $\mathbb{R}X$. Let X_0 be the subgroup of X generated by x_1, \dots, x_{m-1} , then by the induction hypothesis, we have

$$X_0 = \mathbb{Z}x_1 + \dots + \mathbb{Z}x_{m-1}$$

Also, let X' be the subset of X consisting of elements of the form

$$a_1x_1 + \dots + a_mx_m$$

where $0 \leq a_i < 1$ for $i = 1, \dots, m - 1$ and $0 \leq a_m \leq 1$ with $a_i \in \mathbb{R}$. The constraints make X' into a bounded subset of a discrete set X , hence it is finite. We choose $x' \in X'$ with

$$x' = a'_1x_1 + \dots + a'_mx_m$$

such that the coefficient of x_m is minimal, i.e. $|a'_m|$ is minimal. Choose an arbitrary element $x \in X$, then there exists $t \in \mathbb{Z}$ such that $x - tx'$ has its m -th coefficient a_m satisfy $0 \leq a_m < a'_m$. There exists $x_0 \in X_0$ such that $x - tx' - x_0 \in X'$. Because $|a'_m|$ was minimal, we have that $a_m = 0$, hence $x - tx' - x_0 \in X_0$. By the restriction $0 \leq a_i < 1$, we see that $x - tx' - x_0 = 0$. We have already established linear independence, so we have shown that

$$X = \mathbb{Z}x_1 \oplus \dots \oplus \mathbb{Z}x_n$$

as desired. \square

Let W be the \mathbb{R} -span of $\log(k_S)$. Because $\log(k_S) \subset W$, there exists an induced epimorphism

$$\log : \mathbb{I}_S^0 / k_S = C_S^0 \rightarrow H/W$$

We have proved that \mathbb{I}_k^0 is closed, so taking the subspace topology and the quotient topology, we see that C_S^0 is a closed subset of C_k^0 . \log is continuous implies that H/W is a compact subset of \mathbb{R}^n for some n .

Suppose that X is a compact subset of \mathbb{R}^n . X is then of the form

$$X = X_1 \times \cdots \times X_n$$

As projection maps are continuous by definition, X_i are compact. X_i is a subgroup of \mathbb{R} , hence it is either discrete or dense in \mathbb{R} . X_i discrete implies that X_i is discrete and compact, i.e. finite. The only finite subgroup of \mathbb{R} is 0. If X_i is dense in \mathbb{R} , then X_i compact implies that X_i closed. $X_i = \mathbb{R}$, i.e. we have that X is of the form \mathbb{R}^l for some l . \mathbb{R}^l is compact if and only if $l = 0$. $H/W = 0 \Rightarrow H = W$.

We have proved that $\log(k_S)$ has rank $s - 1$. The map $\log : k_S \rightarrow \log(k_S)$. Then the kernel is $x \in k$ such that $\varphi_v(x) = 1$ for v archimedean valuation. The image of the kernel is thus bounded, so by similiar argument, the kernel is finite. Hence k_S and $\log(k_S)$ have the same rank. \square

APPENDIX A. LEMMAS

Proposition A.1 (Reverse Triangle Inequality). *Let φ be a valuation of a field F with $||\varphi|| \leq 2$, then we have*

$$|\varphi(x) - \varphi(y)| \leq \varphi(x - y)$$

where $| \cdot |$ is the usual absolute value of \mathbb{R} .

Proof. For any $x, y \in F$,

$$\varphi(y) = \varphi(y - x + x) \leq \varphi(y - x) + \varphi(x)$$

which implies

$$\varphi(y) - \varphi(x) \leq \varphi(x - y)$$

then by symmetry we get

$$|\varphi(x) - \varphi(y)| \leq \varphi(x - y)$$

\square

Lemma A.2. *Let $a_1, \dots, a_n, b \in \mathbb{R}^{\geq 0}$ with $b \in (b_1, b_2)$, then there exists $\varepsilon \in \mathbb{R}^{>0}$ such that if*

$$\prod_{i=1}^n a_i = b$$

then

$$b_1 < \prod_{i=1}^n a_i - \varepsilon \quad \text{and} \quad \prod_{i=1}^n a_i + \varepsilon < b_2$$

Proof. Let $0 < \gamma < \min(|b_1 - b|, |b_2 - b|)$ and define $\varepsilon = \min(l, \gamma)$ with l to be defined later then

$$\begin{aligned} \prod_{i=1}^n a_i + \varepsilon &= \prod_{i=1}^n a_i + \varepsilon \sum_{j=1}^m \varepsilon^{e_{\varepsilon,j}} a_1^{e_{1,j}} \cdots a_n^{e_{n,j}} \\ &\leq b + \varepsilon l \\ &\quad (l = \sum_{i=1}^m a_1^{e_{1,i}} \cdots a_n^{e_{n,i}}) \\ &\leq b + \frac{\gamma}{l} l \\ &\leq b + \gamma < b_2 \end{aligned}$$

similarly we have that

$$\begin{aligned} \prod_{i=1}^n a_i - \varepsilon &\geq \prod_{i=1}^n a_i + \varepsilon \sum_{i=1}^m (-\varepsilon)^{e_{\varepsilon,i}} a_1^{e_{1,i}} \cdots a_n^{e_{n,i}} \\ &\geq a_i - \varepsilon l \\ &\geq a_i - \frac{\gamma}{l} l \\ &\geq a_i - \gamma > b_1 \end{aligned}$$

which concludes the proof. \square

Proposition A.3. *Let K/F be finite and $x \in K$. $T_x : K \rightarrow K$ be a F -vector space homomorphism defined by $y \mapsto xy$. If f is the characteristic polynomial of T_x and g be the minimal polynomial of x over F , then $f = g^d$ where $d = [K : F(x)]$.*

Proof. We have a simple tower

$$K/F(x)/F$$

let $m = [F(x) : F]$, then $1, x, \dots, x^{m-1}$ is its basis. Also let w_1, \dots, w_d be the $F(x)$ -basis of K . This gives us

$$w_1, w_1x, \dots, w_1x^{m-1}; \dots; w_d, w_dx, \dots, w_dx^{m-1}$$

a F -basis of K . Let $g(t) = t^m + c_1t^{m-1} + \dots + c_m$. Then the matrix representation of T_x with respect to such basis is a block matrix on the diagonal with each block

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \ddots & 1 \\ -c_m & -c_{m-1} & -c_{m-2} & \cdots & -c_1 \end{pmatrix}$$

the characteristic polynomial is then

$$\begin{vmatrix} t & -1 & 0 & \cdots & 0 \\ 0 & t & -1 & \cdots & 0 \\ 0 & 0 & t & \ddots & 1 \\ c_m & c_{m-1} & c_{m-2} & \cdots & c_1 \end{vmatrix} = t \begin{vmatrix} t & -1 & \cdots & 0 \\ 0 & t & \cdots & \vdots \\ \vdots & \vdots & \ddots & -1 \\ c_m & c_{m-2} & \cdots & c_1 \end{vmatrix} - (-1) \begin{vmatrix} 0 & -1 & \cdots & 0 \\ 0 & t & \cdots & \vdots \\ \vdots & \vdots & \ddots & -1 \\ c_{m-1} & c_{m-2} & \cdots & c_1 \end{vmatrix}$$

The left determinant is equal to $(t^{m-1} + \dots + c_{m-1})$ by induction, and the right matrix is also by induction simply c_m . The above expression is equal to

$$t(t^{m-1} + \dots + c_{m-1}) + c_m = t^m + c_1t^{m-1} + \dots + c_m$$

Thus have thus shown that $f = g^d$. \square

In particular, if $x \in F$, then the minimal polynomial is $t - x$, hence the characteristic polynomial is $(t - x)^n$ where $n = [K : F]$ as $F(x) = F$. Then the norm which is the determinant is x^n , i.e. $N_F^K(x) = x^n$ for $x \in F$.

APPENDIX B. QUOTES

Ideles and adeles are a basic innovation. In addition to making class-field theory easier to formulate, they have interesting new properties themselves, and are essentially to understanding L-functions, Galois representations, and automorphic forms. A huge amount of current research concerns these topics and their interconnections, which taken together go by the name “non-abelian class field theory” but really have broader interest. (Don Blasius)

When considering the adeles and ideles, it is their topology as much as their algebraic structure that is of interest. Many important results in number theory translate into simple statements about the topologies of the adeles and ideles. For example, the finiteness of the ideal class group and the Dirichlet unit theorem are equivalent to a certain quotient of the ideles being compact and discrete. (Tom Weston)

In classical number theory, one embeds a number field in the Cartesian product of its completions at the archimedean absolute values, i.e. in a Euclidean space. In more recent years (more precisely since Chevalley introduced ideles in 1936, and Weil gave his adelic proof of the Riemann-Roch theorem soon afterwards), it has been found most convenient to take the product over the completions at all absolute values, including the p-adic ones, with a suitable restriction on the components. (Serge Lang)

The role held in local class field theory by the multiplicative group of the base field is taken in global class field theory by the idele class group. The notion of idele is a modification of the notion of ideal. It was introduced by the French mathematician Claude Chevalley (1909-1984) with a view to providing a suitable basis for the important local-to-global principle, i.e., for the principle which reduces problems concerning a number field K to analogous problems for the various completions K_p . Chevalley used the term *ideal element*, which was abbreviated as id. el. (Neukirch)

INDEX

- S -idele class group, 41
- S -units, 41
- \mathfrak{p} -complete, 20
- \mathfrak{p} -completion, 20
- absolute value, 5, 17
- adeles, 39
- archimedean, 16
- canonical norm, 24
- canonical set, 28
- Cauchy complete, 8
- Cauchy sequence, 5
- compact, 3
- converge, 2
- covers, 3
- Dedekind complete, 8
- dense, 2
- discrete, 18
- discrete set, 2
- equivalent, 16
- exponential valuation, 17
- Hausdorff space, 2
- idele class group, 41
- ideles, 39
- isolated point, 2
- lies over, 35
- limit point, 2
- locally compact, 4
- maximal ideal, 30
- multiplicative valuation, 17
- negative, 8
- neighborhood, 2
- nonarchimedean, 16
- norm, 12
- normalized, 18
- normed, 24
- null sequences, 6, 21
- open cover, 3
- open subcover, 3
- place, 16
- positive, 8
- prime divisor, 16
- product topology, 3
- quotient space, 3
- quotient topology, 3
- restricted product, 38
- topological field, 5
- topological group, 5
- topological ring, 5
- trivial valuation, 11
- unit group, 30
- valuation, 11
- valuation ring, 30

REFERENCES

- [1] Keith Conrad, *Ostrowski for number fields*,
<http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/ostrowski.pdf>
- [2] Andrew Sutherland, *18.905 Lecture Series in Mathematics Lecture #1*,
<http://math.mit.edu/classes/18.095/2015IAP/lecture1/padic.pdf>
- [3] Todd Kemp, *Construction of the real numbers*,
http://ocw.mit.edu/courses/mathematics/18-100b-analysis-i-fall-2010/readings-notes/MIT18_100BF10_Const_of_R.pdf
- [4] Edwin Weiss, *Algebraic Number Theory*. McGraw-Hill Book Company, Inc, 1963.
- [5] Tom Weston, *The Idelic Approach to Number Theory*,
<http://people.math.umass.edu/~weston/oldpapers/idele.pdf>
- [6] Jurgen Neukirch, *Algebraic Number Theory*, Springer-Verlag Berlin Heidelberg New York, 1999.
- [7] Todd Trimble, *nLab: Locally Compact Spaces*,
<https://ncatlab.org/nlab/show/locally+compact+topological+space>
- [8] Walter Rudin, *Principles of Mathematical Analysis*, McGraw-Hill, Inc, 3rd, 1976.
- [9] Terrence Tao, *Locally compact topological vector spaces*,
<https://terrytao.wordpress.com/2011/05/24/locally-compact-topological-vector-spaces/>
E-mail address: libofmath@gmail.com